

MODULARITY OF THE CONSANI-SCHOLTEN QUINTIC

LUIS DIEULEFAIT, ARIEL PACETTI, AND MATTHIAS SCHÜTT

with an Appendix by José Burgos Gil and Ariel Pacetti

ABSTRACT. We prove that the Consani-Scholten quintic, a Calabi-Yau threefold over \mathbb{Q} , is Hilbert modular. For this, we refine several techniques known from the context of modular forms. Most notably, we extend the Faltings-Serre-Livné method to induced four-dimensional Galois representations over \mathbb{Q} . We also need a Sturm bound for Hilbert modular forms; this is developed in an appendix by José Burgos Gil and the second author.

CONTENTS

1. Introduction	2
2. Computing the residual image of the Galois representation $\sigma_{f,2}$	4
3. Computing the residual image of the Galois representation σ_2	8
3.1. Setup	8
3.2. Lefschetz fixed point formula	10
3.3. Proof of Lemma 3.4	11
3.4. Proof of Lemma 3.5	13
4. Proof of the Main Theorem	14
Appendix A. Counting points	18
Appendix B. Sturm Bound (by José Burgos Gil and Ariel Pacetti)	20
B.1. Desingularization and a Sturm bound over \mathbb{C}	20
B.2. Moduli interpretation and integral models	24
B.3. The case the form $(f + \tau(f)) \otimes \chi_{\sqrt{5}}$ of level $\Gamma_0(6\sqrt{5})$	29
References	32

2000 *Mathematics Subject Classification*. Primary: 11F41; Secondary: 11F80, 11G40, 14G10, 14J32.

Key words and phrases. Consani-Scholten quintic, Hilbert modular form, Faltings–Serre–Livné method, Sturm bound.

AP was partially supported by PICT 2006-00312 and UBACyT X867.

MS was partially supported by DFG under grant Schu 2266/2-2.

JBG was partially supported by grants MTM2009-14163-c02-01 and CSIC-2009501001.

1. INTRODUCTION

The modularity conjecture for Calabi-Yau threefolds defined over \mathbb{Q} is a particular instance of the Langlands correspondence. Given a Calabi-Yau threefold X over \mathbb{Q} we consider the compatible family of Galois representations ρ_ℓ of dimension, say, n , giving the action of $G_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $H^3(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$: the conjecture says that there should exist an automorphic form π of GL_n such that ℓ -adic Galois representations attached to π are isomorphic to the ρ_ℓ . This implies that the L -functions of π and ρ_ℓ agree, at least up to finitely many local factors. Observe that (according to Langlands functoriality) π should be cuspidal if and only if the representations ρ_ℓ are absolutely irreducible.

The only case where the conjecture is known in general (among Calabi-Yau threefolds) is the rigid case, i.e., the case with $n = 2$. In this case modularity was established by the first author and Manoharmayum (cf. [DM03]) under some mild local conditions. These local assumptions are no longer required since it is known that modularity of all rigid Calabi-Yau threefolds defined over \mathbb{Q} follows from Serre's conjecture and the latter has recently been proved (cf. [KW09b], [KW09a]). It was observed by Hulek and Verrill in [HV06] that the modularity result in [DM03] can be extended to show modularity of those Calabi-Yau threefolds such that the representations ρ_ℓ are (for every ℓ) reducible and have 2-dimensional irreducible components. In fact, using Serre's conjecture, one can show that this is true even if reducibility occurs only after extending scalars, assuming that reducibility is a uniform property, i.e., independent of ℓ (this uniformity follows for instance from Tate's conjecture).

In this paper, we will prove modularity for a non-rigid Calabi-Yau threefold over \mathbb{Q} such that the representations ρ_ℓ are absolutely irreducible. To our knowledge such an example has not been known before. We sketch the basic set-up:

In [CS01], Consani and Scholten consider a quintic threefold \tilde{X} which we will review in section 3. It has good reduction outside the set $\{2, 3, 5\}$ and Hodge numbers:

$$h^{3,0} = 1 = h^{2,1}, \quad h^{2,0} = 0 = h^{1,0} \text{ and } h^{1,1} = 141.$$

In particular the third étale cohomology is four dimensional. If we fix a prime ℓ , the action of the Galois group $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the third étale cohomology gives a 4-dimensional representation

$$\rho: \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \mapsto \text{GL}(H^3(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)) \simeq \text{GL}_4(\mathbb{Q}_\ell).$$

Let $F = \mathbb{Q}[\sqrt{5}]$ and \mathcal{O}_F its ring of integers. In [CS01] it is shown that the restriction

$$\rho|_{\text{Gal}(\bar{\mathbb{Q}}/F)}: \text{Gal}(\bar{\mathbb{Q}}/F) \mapsto \text{Aut}\left(H^3(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell) \otimes \mathbb{Q}_\ell(\sqrt{5})\right),$$

is the direct sum of two 2-dimensional representations (see Theorem 3.2 of [CS01]). This implies that if λ is a prime of \mathcal{O}_F over ℓ , then there exists a 2-dimensional

representation

$$\sigma_\lambda: \text{Gal}(\bar{\mathbb{Q}}/F) \mapsto \text{GL}_2(\mathcal{O}_\lambda),$$

such that $\rho|_{\text{Gal}(\bar{\mathbb{Q}}/F)}$ is a direct sum of σ and σ' (the conjugate of σ) and $\rho = \text{Ind}_F^{\mathbb{Q}} \sigma$.

In the same work, an holomorphic Hilbert newform \mathfrak{f} on F of weight $(2, 4)$ and conductor $\mathfrak{c}_\mathfrak{f} = (30)$ is constructed, whose L -series is conjectured to agree with that of σ . The aim of this work is to prove this modularity result.

Let λ be a prime of F over a rational prime ℓ . Let \mathcal{O}_λ denote the completion at λ of \mathcal{O}_F . Since \mathfrak{f} has F -rational eigenvalues, by the work of Taylor (see [Tay89]), there exists a two-dimensional continuous λ -adic Galois representation

$$\sigma_{\mathfrak{f},\lambda}: \text{Gal}(\bar{\mathbb{Q}}/F) \mapsto \text{GL}_2(\mathcal{O}_\lambda),$$

with the following properties: $\sigma_{\mathfrak{f},\lambda}$ is unramified outside $\lambda\mathfrak{c}$, and if \mathfrak{p} is a prime of F not dividing $\lambda\mathfrak{c}$, then

$$\text{Tr } \sigma(\text{Frob } \mathfrak{p}) = \theta(T_\mathfrak{p}),$$

$$\det \sigma(\text{Frob } \mathfrak{p}) = \theta(S_\mathfrak{p})\mathcal{N}\mathfrak{p}.$$

Here $T_\mathfrak{p}$ denotes the \mathfrak{p} -th Hecke operator, $S_\mathfrak{p}$ denotes the diamond operator (given by the action of the matrix $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$, for $\alpha = \prod_{\mathfrak{q}} \pi_{\mathfrak{q}}^{v_{\mathfrak{q}}(\mathfrak{p})}$ and $\pi_{\mathfrak{q}}$ a local uniformizer) and $\theta(T)$ is the eigenvalue of \mathfrak{f} at the operator T . There is also information about the behaviour at the ramified primes. This allows us to compare the 2-dimensional Galois representations $\sigma_\lambda, \sigma_{\mathfrak{f},\lambda}$. Let \mathfrak{f}^τ be the Hilbert modular form which is the Galois conjugate of \mathfrak{f} , where τ is the order two element in $\text{Gal}(F/\mathbb{Q})$. The λ -adic Galois representations attached to \mathfrak{f}^τ are precisely the Galois conjugates of those attached to \mathfrak{f} . Our result can be stated as:

Theorem 1.1. *The representations σ_λ and $\sigma_{\mathfrak{f}^\tau,\lambda}$ are isomorphic, where τ is either the identity or τ .*

In particular the theorem implies that the L -series of σ_λ and $\sigma_{\mathfrak{f}^\tau,\lambda}$ agree. This solves the conjecture from [CS01].

Remark 1.2. By known cases of automorphic base change (theta lift) and functoriality, Theorem 1.1 is known to imply that ρ corresponds to a Siegel modular form of genus 2 and to a cuspidal automorphic form of GL_4 .

Remark 1.3. Dimitrov has proved a Modularity Lifting Theorem that applies to Hilbert modular forms of non-parallel weight (cf. [Dim09]), and he and the first author checked that for $\ell = 7$ the representation σ satisfies all the technical conditions of this theorem (cf. [DD06]). Thus it would be enough to prove residual modularity modulo 7 to deduce the modularity of σ from this result. We will follow, however, a different path.

We give an outline of the proof of Theorem 1.1. Since both Galois representations come in compatible families, it is enough to prove that they are isomorphic for a specific choice of primes ℓ and λ over ℓ . We choose $\ell = 2$ so as to apply

a Faltings-Serre method of proving that two given 2-adic Galois representations are isomorphic (cf. [Liv87]). Actually, in [CS01] it is proven that σ_λ exists, but there is no natural choice to distinguish its trace at a prime from its conjugate trace, so in Theorem 4.3 we give a version of Faltings-Serre result that applies to the 4-dimensional representations.

Such theorem implies that both representations have isomorphic semisimplifications, but since \mathfrak{f} is a cuspidal Hilbert eigenform, its λ -adic Galois representations is irreducible for all primes λ and Livné's Theorem asserts in particular that the same is true for the representations attached to \tilde{X} .

In the present situation, the main problem comes from the fact that 2 is inert in \mathcal{O}_F . Hence the residual representations lie a priori in $\mathrm{GL}_2(\mathbb{F}_4)$. Actually, it lies in $\mathrm{SL}_2(\mathbb{F}_4)$. This is clear for both representations: the representation $\sigma_{\mathfrak{f},\lambda}$ has trivial nebentypus so the determinant image lies in \mathbb{F}_2 while the representation σ_λ at a prime ideal \mathfrak{p} has real determinant of absolute value $N\mathfrak{p}^3$.

The group $\mathrm{SL}_2(\mathbb{F}_4)$ is not a solvable group (it is in fact isomorphic to A_5 , the alternating group in 5 elements). We will overcome this subtlety by showing that the images of the residual representations are 2-groups. For $\sigma_{\mathfrak{f},2}$, this will be achieved in section 2 by combining two techniques: the explicit approach from [DGP] and a Sturm bound for Hilbert modular forms that is developed by Burgos and the second author in the Appendix B. For σ_2 , we will use the Lefschetz trace formula and automorphisms on the Calabi-Yau threefold \tilde{X} (section 3). We collect the necessary data for a proof of Theorem 1.1 in section 4.

Acknowledgements: We would like to thank Lassina Démbélé for many suggestions concerning computing with Hilbert modular forms. Also we would like to thank José Burgos Gil for his contribution to the appendix with the proof of a Sturm bound. The computations of the $a_{\mathfrak{p}}$ where done using the Pari/GP system [PAR08]. We would like to thank Bill Allombert for implementing a routine in PARI that was not included in the original software for dealing with elements of small norm under a positive definite quadratic form.

2. COMPUTING THE RESIDUAL IMAGE OF THE GALOIS REPRESENTATION $\sigma_{\mathfrak{f},2}$

The aim of this section is to prove that the image of the residual 2-adic Galois representation attached to \mathfrak{f} has image a 2-group. Eventually we will pursue a similar approach as in [DGP]. We start by computing all subgroups of A_5 .

Lemma 2.1. *Any proper subgroup of A_5 is isomorphic to one of the following:*

$$\{\{1\}, C_2, C_3, C_2 \times C_2, C_5, S_3, D_5, A_4\}.$$

Proof. This is a standard computation (also some software like Gap computes the subgroups of a small permutation group). \square

There is an easy classification of the orders of the elements in $\mathrm{SL}_2(\mathbb{F}_4)$ in terms of the traces.

Lemma 2.2. *If $M \in \mathrm{SL}_2(\mathbb{F}_4)$, then*

$$\mathrm{ord}(M) = \begin{cases} 1 & \text{if } M = \mathrm{id}, \\ 2 & \text{if } \mathrm{Tr}(M) = 0 \text{ and } M \neq \mathrm{id}, \\ 3 & \text{if } \mathrm{Tr}(M) = 1, \\ 5 & \text{if } \mathrm{Tr}(M) \notin \mathbb{F}_2. \end{cases}$$

Proof. The proof is quite elementary, so we leave it to the reader. \square

Proposition 2.3. *The residual image of $\sigma_{f,2}$ does not contain order 5 elements.*

To prove this proposition, we use the Sturm bound for Hilbert modular forms proved in Appendix B. Recall how to derive a Fourier expansion at ∞ for a Hilbert modular form over F . Let τ denote the generator of $\mathrm{Gal}(F/\mathbb{Q})$. An element $\nu \in F$ is called totally positive if both $\nu > 0$ and $\tau(\nu) > 0$. We denote this by $\nu \gg 0$. Since F has class number one, any Hilbert modular form G over F can be written as double sum over ideals \mathfrak{b} of \mathcal{O}_F and totally positive elements $\nu \in \mathfrak{b}/\sqrt{5}$

$$(1) \quad G(z_1, z_2) = \sum_{\mathfrak{b} \subset \mathcal{O}_F} a_{\mathfrak{b}} \left(\sum_{\substack{\xi \in \frac{\mathfrak{b}}{\sqrt{5}} \\ \xi \gg 0}} \exp(\xi z_1 + \tau(\xi) z_2) \right),$$

where $\exp(z) = e^{2\pi i z}$. The main result of Appendix B (Theorem B.25) reads

Theorem. *Assume that a Hilbert cusp form of weight $(2, 4)$ for $\Gamma_0(6\sqrt{5})$ has a q -expansion at ∞ which satisfies $a_{\xi} \in 2\mathcal{O}_F$ for all totally positive elements $\xi \in \mathcal{O}_F^{\vee}$ with $\mathrm{Tr}(\xi) \leq 168$. Then all its Fourier coefficients are in $2\mathcal{O}_F$.*

If the Hilbert modular form G in (1) is a normalized eigenform, then the eigenvalue of the Hecke operator $T_{\mathfrak{p}}$ is given by $a_{\mathfrak{p}}$. A way to compute the a_{ξ} up to the bound is to use equation (1) and compute the elements associated to prime ideals (since our form has an Euler product). The relation between the ideal norm and the trace is given by the following.

Lemma 2.4. *Let \mathfrak{b} be an ideal of \mathcal{O}_K of norm $N(\mathfrak{b})$. Then if $\nu \in \frac{\mathfrak{b}}{\sqrt{5}}$ is totally positive, $\mathrm{Tr}(\nu) \geq \sqrt{\frac{4}{5}} \sqrt{N(\mathfrak{b})}$.*

Proof. Say $\nu = \frac{5b+a\sqrt{5}}{10}$, with $a, b \in \mathbb{Z}$ and $a \equiv b \pmod{2}$. Clearly, $\mathrm{Tr}(\nu) = b$, while its norm is

$$N(\nu) = \frac{5b^2 - a^2}{20} \geq \frac{N(\mathfrak{b})}{5}.$$

Then $\frac{b^2}{4} = N(\nu) + \frac{a^2}{20} \geq N(\nu) \geq \frac{N(\mathfrak{b})}{5}$, so $\mathrm{Tr}(\nu) \geq \sqrt{\frac{4}{5}} \sqrt{N(\mathfrak{b})}$. \square

Lemma 2.5. *There exists a unique non-trivial quadratic Hecke character $\chi_{\sqrt{5}}$ of \mathcal{O}_F (of infinity type $(0,0)$), whose conductor is $\sqrt{5}$. The quadratic twist of \mathfrak{f} by $\chi_{\sqrt{5}}$ corresponds to a Hilbert newform of level $6\sqrt{5}$ and weight $(2,4)$ which we denote by $\mathfrak{f} \otimes \chi_{\sqrt{5}}$.*

Proof. The fact that the fundamental unit is not totally positive allows for any prime ideal \mathfrak{p} of \mathcal{O}_F whose residue field has prime order p to define such a Hecke character. It is given by composing of the maps

$$\mathcal{O}_F \twoheadrightarrow \mathcal{O}_F/\mathfrak{p} \simeq \mathbb{F}_p \xrightarrow{\left(\frac{-}{p}\right)} \{\pm 1\}.$$

For the second statement of the Lemma, it is clear that (as in the classical case) the twist will have level at most 30 (see for example [Car86]). Then the proof continues by elimination. We computed the space of newforms of level 30, and there are 16 eigenforms whose coefficient field is F . We computed the quadratic twist of the form \mathfrak{f} and it is not in this newspace. Hence we search for it in the newspace of level 6 (which has dimension 2) and in the newspace of level $6\sqrt{5}$ (which has dimension 4), and we found the form in the latter. The computation of these spaces was carried out by Lassina Démbélé. \square

Proof of Proposition 2.3: Suppose the residual image of $\sigma_{\mathfrak{f},2}$ contains an element of order 5. Then by Lemma 2.2 there exists a prime \mathfrak{p}_0 such that the \mathfrak{p}_0 -th Hecke eigenvalue $a_{\mathfrak{p}_0}$ lies in \mathbb{F}_4 , but not in \mathbb{F}_2 . Consider the form $\mathfrak{f} + \tau(\mathfrak{f})$, where τ is the generator of $\text{Gal}(F/\mathbb{Q})$. It is a weight $(2,4)$ Hilbert modular form, whose \mathfrak{p}_0 -th Fourier coefficient is non-zero modulo 2. Then Lemma 2.5 implies that its twist by the character $\chi_{\sqrt{5}}$ is a Hilbert newform of weight $(2,4)$ and level $6\sqrt{5}$ whose \mathfrak{p}_0 -th Fourier coefficients is non-zero as well.

We computed all Hecke eigenvalues with ideals generated by an element of trace smaller than 168 of \mathfrak{f} and checked that they all lie in $2\mathcal{O}_F$ (a table for such eigenvalues can be found at [DPS]). In particular, all the Fourier coefficients of the Hilbert modular form $(\mathfrak{f} + \tau(\mathfrak{f})) \otimes \chi_{\sqrt{5}}$ with trace smaller than 168 are zero modulo $2\mathcal{O}_F$. Theorem B.25 then implies that all Fourier coefficients are in fact zero modulo $2\mathcal{O}_F$, which contradicts the fact that its \mathfrak{p}_0 -th coefficient is not. \square

Remark 2.6. The same approach as above could be pursued for the original Hilbert modular form of level 30. Then the Sturm bound would require to verify the parity of the Fourier coefficients for all totally positive elements $\xi \in \mathcal{O}_F^\vee$ with $\text{Tr}(\xi) \leq 850$.

It remains to prove that the residual image at 2 cannot be any of the groups $\{C_3, S_3, A_4\}$. We recall some well known results from Class Field Theory:

Theorem 2.7. *If L/F is an abelian Galois extension unramified outside the set of places $\{\mathfrak{p}_i\}_{i=1}^n$ then there exists a modulus $\mathfrak{m} = \prod_{i=1}^n \mathfrak{p}_i^{e(\mathfrak{p}_i)}$ such that $\text{Gal}(L/F)$ corresponds to a subgroup of the ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$.*

A bound for $e(\mathfrak{p})$ is given by the following result.

Proposition 2.8. *Let L/F be an abelian Galois extension of prime degree p . Consider a modulus $\mathfrak{m} = \prod_{i=1}^n \mathfrak{p}_i^{e(\mathfrak{p}_i)}$ associated to the extension L/F by Theorem 2.7. If \mathfrak{p} ramifies in L/F , then*

$$\begin{cases} e(\mathfrak{p}) = 1 & \text{if } \mathfrak{p} \nmid p \\ 2 \leq e(\mathfrak{p}) \leq \left\lfloor \frac{pe(\mathfrak{p}|p)}{p-1} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid p, \end{cases}$$

where \mathfrak{p} is a prime above the rational prime p and $e(\mathfrak{p}|p)$ is the ramification index of \mathfrak{p} in F/\mathbb{Q} .

Proof. See [Coh00] Proposition 3.3.21 and Proposition 3.3.22. \square

Using these two results, we can compute for each possible Galois group all Galois extensions of F unramified outside $\{2, 3, 5\}$. In each extension, we find a prime \mathfrak{p} where the Frobenius has non-zero trace (in \mathbb{F}_4). If $a_{\mathfrak{p}} \equiv 0 \pmod{2}$, for all such primes we are done:

Proposition 2.9. *The residual representation $\bar{\sigma}_{f,2}$ has image a 2-group.*

Proof. Consider the different cases:

- The group A_4 has $C_2 \times C_2$ as a normal subgroup (with generators (12)(34) and (13)(24)). The quotient by this subgroup is a cyclic group of order 3, so the extension contains a cubic Galois subfield. Since there are no elements of order 6 in A_4 , a non trivial element in this Galois group will have odd trace. Thus the case A_4 and C_3 can be discarded at the same time.

In order to do so, we can take $\mathfrak{m} = 2 \cdot 3^2 \cdot \sqrt{5}$ as the maximal modulus by Proposition 2.9. The ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $C_{12} \times C_6$ so there are 4 cubic extensions ramified at these primes. We consider the characters as additive characters (by taking logarithms), and denote by ψ_1 and ψ_2 two characters that generate the group of characters of order 3 (we take the fourth and the second power of the characters in the previous basis). Instead of computing a prime ideal where each character is non-zero, we compute two prime ideals \mathfrak{p}_1 and \mathfrak{p}_2 such that

$$\langle (\psi_1(\mathfrak{p}_1), \psi_2(\mathfrak{p}_1)), (\psi_1(\mathfrak{p}_2), \psi_2(\mathfrak{p}_2)) \rangle = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Then Proposition 5.4 of [DGP] implies that any cubic character is non-trivial in one of these two ideals. The two ideals above the prime 11 have values (1, 0) and (1, 2), which is a basis for $\mathbb{F}_3 \times \mathbb{F}_3$. Since the modular form has even traces (in \mathbb{F}_2) at both primes (see Table of [CS01]), we conclude that the residual representation cannot have image isomorphic to C_3 nor A_4 .

- To discard the S_3 case, we start by computing all the quadratic extensions of F ramified outside the set of primes $\{2, 3, 5\}$. The modulus in this case is $\mathfrak{m} = 2^3 \cdot 3 \cdot \sqrt{5}$. The ray class group is isomorphic to $C_4 \times C_4 \times C_2 \times C_2 \times C_2$

so there are 31 such extensions. In Table 2.1 we put all the information of these extensions; the first column has an equation for each such extension, the second column its discriminant over \mathbb{Q} , the third column the modulus considered (where by \mathfrak{p}_2 (respectively \mathfrak{p}_5) we denote the unique prime ideal in the extension above the rational prime 2 (respectively 5)), the fourth column the ray class group and the last column the rational primes whose prime divisors in F generate the \mathbb{F}_3 vector space of cubic characters.

Note that the first 16 extensions are not Galois over \mathbb{Q} and are listed so that they are isomorphic in pairs. The last 15 are indeed Galois over \mathbb{Q} . This implies that we could consider one element of each pair for the first fields. Note that the primes at conjugate fields are the same, since the Frobenius at a prime in F of a field is the same as the Frobenius at the conjugate of the prime in the conjugate extension.

The traces of Frobenius are even in all such primes (see Table of [CS01]), so we conclude that the image of the residual representation $\bar{\sigma}_{f,2}$ cannot be isomorphic to S_3 either. \square

3. COMPUTING THE RESIDUAL IMAGE OF THE GALOIS REPRESENTATION σ_2

In this section we consider the Consani-Scholten Quintic \tilde{X} from [CS01]. Our goal is to prove that the ℓ -adic Galois representations ρ of $H^3(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_{\ell})$ have 4-divisible trace. This will be used to deduce that modulo 2 the restricted 2-adic two-dimensional Galois representations have image in $\mathrm{SL}_2(\mathbb{F}_2)$, so that we can apply the Faltings-Serre-Livné method.

3.1. Setup. Consider the Chebyshev polynomial

$$P(y, z) = (y^5 + z^5) - 5yz(y^2 + z^2) + 5yz(y + z) + 5(y^2 + z^2) - 5(y + z).$$

Then we define an affine variety X in \mathbb{A}^4 by

$$X: P(x_1, x_2) = P(x_4, x_5).$$

Let $\bar{X} \subset \mathbb{P}^4$ denote the projective closure of X . Then \bar{X} has 120 ordinary double points. Let \tilde{X} denote a desingularisation obtained by blowing up \bar{X} at the singularities.

Remark 3.1. We might also consider a small resolution \hat{X} , as many of the nodes lie on products of lines. Then we would have to check that \hat{X} is projective and can be defined over \mathbb{Q} . This desingularisation would have the advantage of producing an honest Calabi-Yau threefold, but it does not affect the question of Hilbert modularity.

Equation over F	Disc. over \mathbb{Q}	Modulus	Ray Class Group	Rational Primes
$x^2 - 6\sqrt{5}$	$-2^6 \cdot 3^2 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{72} \times C_6 \times C_3 \times C_3$	$\{7, 11, 13\}$
$x^2 + 6\sqrt{5}$	$-2^6 \cdot 3^2 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{72} \times C_6 \times C_3 \times C_3$	$\{7, 11, 13\}$
$x^2 + \sqrt{5} + 1$	$-2^6 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{12} \times C_6 \times C_3$	$\{7, 11, 13, 19\}$
$x^2 - \sqrt{5} - 1$	$-2^6 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{12} \times C_6 \times C_3$	$\{7, 11, 13, 19\}$
$x^2 - 3\sqrt{5} - 3$	$-2^6 \cdot 3^2 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{36} \times C_6 \times C_3 \times C_3$	$\{7, 11, 13, 17\}$
$x^2 + 3\sqrt{5} + 3$	$-2^6 \cdot 3^2 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{36} \times C_6 \times C_3 \times C_3$	$\{7, 11, 13, 17\}$
$x^2 + 2\sqrt{5}$	$-2^6 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{24} \times C_6 \times C_3$	$\{7, 11, 13\}$
$x^2 - 2\sqrt{5}$	$-2^6 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{24} \times C_6 \times C_3$	$\{7, 11, 13\}$
$x^2 + \frac{3}{2}\sqrt{5} + \frac{3}{2}$	$-2^4 \cdot 3^2 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{36} \times C_6 \times C_3$	$\{7, 11, 13\}$
$x^2 - \frac{3}{2}\sqrt{5} - \frac{3}{2}$	$-2^4 \cdot 3^2 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{36} \times C_6 \times C_3$	$\{7, 11, 13\}$
$x^2 - \sqrt{5}$	$-2^4 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{24} \times C_6 \times C_3$	$\{7, 11, 13\}$
$x^2 + \sqrt{5}$	$-2^4 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{24} \times C_6 \times C_3$	$\{7, 11, 13\}$
$x^2 + 3\sqrt{5}$	$-2^4 \cdot 3^2 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{24} \times C_6 \times C_3 \times C_3$	$\{7, 11, 13\}$
$x^2 - 3\sqrt{5}$	$-2^4 \cdot 3^2 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{24} \times C_6 \times C_3 \times C_3$	$\{7, 11, 13\}$
$x^2 - \frac{1}{2}\sqrt{5} - \frac{1}{2}$	$-2^4 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{12} \times C_6 \times C_3 \times C_3$	$\{7, 11, 13, 17\}$
$x^2 + \frac{1}{2}\sqrt{5} + \frac{1}{2}$	$-2^4 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{12} \times C_6 \times C_3 \times C_3$	$\{7, 11, 13, 17\}$
$x^2 + \sqrt{5} + 5$	$2^6 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{60} \times C_6 \times C_3 \times C_3$	$\{7, 11, 13, 23\}$
$x^2 - 6$	$2^6 \cdot 3^2 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{12} \times C_6 \times C_6$	$\{7, 11, 13, 23\}$
$x^2 + 2$	$2^6 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{24} \times C_{12} \times C_3 \times C_3 \times C_3$	$\{7, 11, 13, 23\}$
$x^2 - 3\sqrt{5} - 15$	$2^6 \cdot 3^2 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{12} \times C_6$	$\{7, 11, 13\}$
$x^2 + 6$	$2^6 \cdot 3^2 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{72} \times C_{12} \times C_3 \times C_3 \times C_3$	$\{7, 11, 13, 17\}$
$x^2 - \sqrt{5} - 5$	$2^6 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{36} \times C_{18} \times C_3 \times C_3$	$\{7, 11, 13\}$
$x^2 + 3\sqrt{5} + 15$	$2^6 \cdot 3^2 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{12} \times C_6 \times C_6$	$\{7, 11, 13, 61\}$
$x^2 - 2$	$2^6 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{36} \times C_{18} \times C_3 \times C_3$	$\{7, 11, 13\}$
$x^2 + \frac{3}{2}\sqrt{5} + \frac{15}{2}$	$2^4 \cdot 3^2 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{36} \times C_{18} \times C_3 \times C_3$	$\{7, 11, 13\}$
$x^2 + 3$	$3^2 \cdot 5^2$	$18 \cdot \sqrt{5}$	$C_{36} \times C_3 \times C_3 \times C_3 \times C_3 \times C_3$	$\{7, 11, 13, 17, 19, 23\}$
$x^2 + 1$	$2^4 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{24} \times C_{12} \times C_3 \times C_3$	$\{7, 11, 13, 17\}$
$x^2 + \frac{1}{2}\sqrt{5} + \frac{5}{2}$	5^3	$18 \cdot \mathfrak{p}_5$	$C_{60} \times C_3 \times C_3 \times C_3$	$\{7, 11, 13\}$
$x^2 - \frac{1}{2}\sqrt{5} - \frac{5}{2}$	$2^4 \cdot 5^3$	$9 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_5$	$C_{12} \times C_6$	$\{7, 11, 13\}$
$x^2 - 3$	$2^4 \cdot 3^2 \cdot 5^2$	$9 \cdot \mathfrak{p}_2 \cdot \sqrt{5}$	$C_{12} \times C_6 \times C_6 \times C_3$	$\{7, 11, 13\}$
$x^2 - \frac{3}{2}\sqrt{5} - \frac{15}{2}$	$3^2 \cdot 5^3$	$18 \cdot \mathfrak{p}_5$	$C_6 \times C_6$	$\{7, 11, 13\}$

TABLE 2.1. Quadratic extensions of F unramified outside $\{2, 3, 5\}$

Consani and Scholten compute the Hodge diamond of \tilde{X} as follows:

$$\begin{array}{ccccccc}
& & & & 1 & & \\
& & & 0 & & 0 & \\
& & 0 & & 141 & & 0 \\
1 & & 1 & & 1 & & 1 \\
& & 0 & & 141 & & 0 \\
& & 0 & & 0 & & \\
& & & & 1 & &
\end{array}$$

Hence the étale cohomology groups $H^3(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$ (ℓ prime) give rise to a compatible system of four-dimensional Galois representations $\{\rho_\ell\}$. Since \tilde{X} has good reduction outside $\{2, 3, 5\}$, ρ_ℓ is unramified outside $\{2, 3, 5, \ell\}$.

Let $F = \mathbb{Q}(\sqrt{5})$ and fix some prime $\ell \in \mathbb{N}$ and $\lambda \in F$ above ℓ . Then Consani and Scholten prove for the ℓ - resp. λ -adic representations:

Theorem 3.2 (Consani-Scholten). *The restriction $\rho|_{\text{Gal}(\bar{\mathbb{Q}}/F)}$ is reducible as a representation into $\text{GL}_4(F_\lambda)$: There is a Galois representation*

$$\sigma: \text{Gal}(\bar{\mathbb{Q}}/F) \rightarrow \text{GL}_2(F_\lambda)$$

such that $\rho = \text{Ind}_F^{\mathbb{Q}} \sigma$.

Here we want to prove the following property:

Proposition 3.3. *The Galois representation ρ has 4-divisible trace.*

In fact, for $q \equiv 2, 3 \pmod{5}$, Consani-Scholten proved that $\rho(\text{Frob}_q)$ has zero trace. Hence we would only have to consider the case $q \equiv 1, 4 \pmod{5}$, although we will treat the problem in full generality.

As a corollary, we deduce the according divisibility of σ .

3.2. Lefschetz fixed point formula. Choose a prime $p \neq \ell$ of good reduction for \tilde{X} and let $q = p^r$. Consider the geometric Frobenius endomorphism Frob_q on \tilde{X}/\mathbb{F}_p , raising coordinates to their q -th powers. Then the Lefschetz fixed point formula tells us that

$$\#\tilde{X}(\mathbb{F}_q) = \sum_{i=0}^6 (-1)^i \text{trace } \text{Frob}_q^*(H^i(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)).$$

In our situation, this simplifies as follows: $h^1 = h^5 = 0$; $H^2(\tilde{X})$ and $H^4(\tilde{X})$ are algebraic by virtue of the exponential sequence and Poincaré duality. Moreover Frob_q^* factors through a permutation on $H^2(\tilde{X})$, i.e. all eigenvalues have the shape ζq where ζ is some root of unity. Denote the sum of these roots of unity by h_q (which is an integer in \mathbb{Z} by the Weil conjectures). Finally geometric and algebraic Frobenius are compatible through ρ . Hence

$$(2) \quad \text{trace } \rho(\text{Frob}_q) = 1 + h_q q(1 + q) + q^3 - \#\tilde{X}(\mathbb{F}_q).$$

Prop. 3.3 claims that the left hand side is divisible by 4. If $q \equiv -1 \pmod{4}$, this is a consequence of the following

Lemma 3.4. *For any good prime p and $q = p^r$, $\#\tilde{X}(\mathbb{F}_q) \equiv 0 \pmod{4}$.*

If $q \equiv 1 \pmod{4}$, then we furthermore need the following

Lemma 3.5. *For any good prime p and $q = p^r$, h_q is odd.*

3.3. Proof of Lemma 3.4. To prove Lemma 3.4, we use the action of the dihedral group D_4 on \tilde{X} and the knowledge about the exceptional divisors from Consani-Scholten.

Let ζ_n denote a primitive n -th root of unity. Then all the nodes are defined over $\mathbb{Q}(\zeta_{15})$. A detailed list can be found in [CS01]. Over the field of definition of the node, the exceptional divisor E is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$. Hence $\#E(\mathbb{F}_q) = (q+1)^2$ if the node is defined over \mathbb{F}_q .

Lemma 3.6. *For any good prime p and $q = p^r$, $\#\tilde{X}(\mathbb{F}_q) \equiv \#\bar{X}(\mathbb{F}_q) \pmod{32}$.*

Proof: By [CS01], we have

$$\#\{\text{nodes over } \mathbb{F}_q\} = \begin{cases} 0, & q \equiv 2, 7, 8, 13 \pmod{15}, \\ 8, & q \equiv 14 \pmod{15}, \\ 24, & q \equiv 4 \pmod{15}, \\ 104, & q \equiv 11 \pmod{15}, \\ 120, & q \equiv 1 \pmod{15}. \end{cases}$$

Since the number of points on the exceptional divisor is the same for all nodes defined over \mathbb{F}_q , the claim follows. \square

Lemma 3.7. *For any good prime p and $q = p^r$, $\#\bar{X}(\mathbb{F}_q) \equiv \#X(\mathbb{F}_q) - q \pmod{4}$.*

Proof: The affine variety X is compactified by adding a smooth surface at ∞ . In fact, this is the Fermat surface of degree five:

$$S = \{x_0^5 + x_1^5 - x_3^5 - x_4^5 = 0\} \subset \mathbb{P}^3.$$

Hence $\#\bar{X}(\mathbb{F}_q) - \#X(\mathbb{F}_q) = \#S(\mathbb{F}_q)$. Thus Lemma 3.7 amounts to the following

Lemma 3.8. *For $p \neq 5$ and $q = p^r$, $\#S(\mathbb{F}_q) \equiv 1 + q + q^2 \pmod{4}$.*

The proof of this lemma will be postponed to the end of this section. Lemma 3.7 follows. \square

To prove the corresponding statement about the affine variety X , we use the action of the dihedral group D_4 generated by the involutions

$$(x_1, x_2, x_3, x_4) \mapsto (x_2, x_1, x_3, x_4), \quad (x_1, x_2, x_3, x_4) \mapsto (x_1, x_2, x_4, x_3)$$

and by the cyclic permutation

$$(3) \quad \gamma: (x_1, x_2, x_3, x_4) \mapsto (x_3, x_4, x_2, x_1).$$

It follows that

$$\#X(\mathbb{F}_q) \equiv \#\{x \in X(\mathbb{F}_q); \#\{y \in (D_4 - \text{orbit of } x)\} < 4\} \pmod{4}.$$

Here $\{x \in X(\mathbb{F}_q); \#\{y \in (D_4 - \text{orbit of } x)\} < 4\} = \{(x_1, x_1, x_3, x_3) \in X(\mathbb{F}_q)\}$. We are led to consider the affine curve C in \mathbb{A}^2 defined by

$$C: \quad P(y, y) = P(z, z).$$

Then the above subset of $X(\mathbb{F}_q)$ is in bijection with $C(\mathbb{F}_q)$, and we obtain

$$(4) \quad \#X(\mathbb{F}_q) \equiv C(\mathbb{F}_q) \pmod{4}.$$

Lemma 3.9. *For any good prime p and $q = p^r$, $\#C(\mathbb{F}_q) \equiv q \pmod{4}$.*

Proof of Lemma 3.9: C is reducible. The change of variables

$$u = \frac{y+z}{2}, \quad v = \frac{y-z}{2}$$

allows us to write

$$P(y, y) - P(z, z) = v(v^4 + 5(2u^2 - 4u + 1)v^2 + 5(u^2 - 3u + 1)(u^2 - u - 1)) = vG(u, v).$$

Hence

$$(5) \quad \#C(\mathbb{F}_q) = q + \#(B(\mathbb{F}_q) \cap \{v \neq 0\})$$

where B is the affine curve in \mathbb{A}^2 given by $G(u, v) = 0$. Here B is endowed with involutions

$$(u, v) \mapsto (u, -v), \quad (u, v) \mapsto (2 - u, v).$$

For the number of points, this implies

$$\begin{aligned} \#(B(\mathbb{F}_q) \cap \{v \neq 0\}) &\equiv \#(B(\mathbb{F}_q) \cap \{u = 1, v \neq 0\}) \pmod{4} \\ &= \#\{v \in \mathbb{F}_q; v^4 - 5v^2 + 5 = 0\}. \end{aligned}$$

The last polynomial factors as

$$4(v^4 - 5v^2 + 5) = (2v^2 - 5 - \sqrt{5})(2v^2 - 5 + \sqrt{5}).$$

Since $\frac{5+\sqrt{5}}{2} \cdot \frac{5-\sqrt{5}}{2} = 4$, a square, we deduce that the last equation has either zero or four solutions in \mathbb{F}_q . In particular, (5) reduces to $\#C(\mathbb{F}_q) \equiv q \pmod{4}$, i.e. to the claim of Lemma 3.9. \square

Proof of Lemma 3.8: We shall again use the cyclic permutation γ from (3), but this time it operates on the homogeneous coordinates of \mathbb{P}^3 . Hence

$$(6) \quad \#S(\mathbb{F}_q) \equiv \#(S \cap \text{Fix}(\sigma^2))(\mathbb{F}_q) \pmod{4}.$$

Here

$$\text{Fix}(\sigma^2) = \{[\lambda, \mu, \pm\lambda, \pm\mu]; [\lambda, \mu] \in \mathbb{P}^1\}.$$

One of these lines is contained in S , and it is easy to see that there are exactly $(5, q - 1)$ further points of intersection unless $p = 2$. I.e.

$$\#(S \cap \text{Fix}(\sigma^2))(\mathbb{F}_q) = 1 + q + \begin{cases} 0, & p = 2 \\ (5, q - 1), & p \neq 2 \end{cases} \equiv 1 + q + q^2 \pmod{4}.$$

Lemma 3.8 follows from this congruence and (6). \square

Proof of Lemma 3.4: Lemma 3.9 and (4) imply that $\#X(\mathbb{F}_q) \equiv q \pmod{4}$. By Lemma 3.7 this gives $\#\bar{X}(\mathbb{F}_q) \equiv 0 \pmod{4}$. The according statement for \tilde{X} is obtained from Lemma 3.6. \square

3.4. Proof of Lemma 3.5. Lemma 3.5 states that the trace h_q of Frob_q on $H^2(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$ is always odd. We shall first prove the following auxiliary result:

Lemma 3.10. *The Galois group $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_{15}))$ acts trivially on $H^2(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$.*

Proof: Denote the exceptional locus of the blow-up by E . Then E is defined over \mathbb{Q} . The Leray spectral sequence for the desingularisation gives an exact sequence

$$(7) \quad 0 \rightarrow H^2(\bar{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1)) \rightarrow H^2(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1)) \rightarrow H^2(E_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1)).$$

By construction, (7) is compatible with the Galois action. Here $H^2(\bar{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$ is the same as for a general quintic hypersurface in \mathbb{P}^4 . Hence it has dimension one and is generated by the class of a hyperplane section. In particular, $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts trivially on $H^2(\bar{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$. Recall that every component of E as well as both rulings on every component are defined over $\mathbb{Q}(\zeta_{15})$. Hence $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_{15}))$ acts trivially on $H^2(E_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$. By the Galois-equivariant exact sequence (7), the same holds for $H^2(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$. \square

It follows from Lemma 3.10, that $h_q = 141$ if $q \equiv 1 \pmod{15}$. To prove the parity for the other residue classes, we need two easy statements about sums of primitive roots of unity. They involve the Möbius function $\mu: \mathbb{N} \rightarrow \{-1, 0, 1\}$:

$$\mu(n) = \begin{cases} 0, & n \text{ not squarefree,} \\ (-1)^m, & n \text{ squarefree with } m \text{ prime divisors.} \end{cases}$$

Lemma 3.11. *Let $n \in \mathbb{N}$ and ζ_n a primitive n -th root of unity. Then ζ_n has trace $\mu(n)$.*

The lemma follows immediately from the factorisation of the cyclotomic polynomial $x^n - 1$ and the definition of $\mu(n)$.

Lemma 3.12. *Let $n \in \mathbb{N}$ and ζ_n a primitive n -th root of unity. Let $m = 2^s \cdot k$ with $(k, n) = 1$. Then*

$$\mu(n) = \text{trace } \zeta_n = \sum_{j \in (\mathbb{Z}/n\mathbb{Z})^*} \zeta_n^j \equiv \sum_{j \in (\mathbb{Z}/n\mathbb{Z})^*} \zeta_n^{mj} \pmod{2}.$$

Proof: If $(m, n) = 1$, then taking m -th powers permutes the primitive n -th roots of unity and both sums coincide. Hence it suffices to consider the case where $m = 2^s (s > 0)$ and $2|n$.

If $4 \nmid n$, then $\{\zeta_n^{mj}; j \in (\mathbb{Z}/n\mathbb{Z})^*\}$ is the set of $\frac{n}{2}$ -th primitive roots of unity. Hence

$$\sum_{j \in (\mathbb{Z}/n\mathbb{Z})^*} \zeta_n^{mj} = \mu\left(\frac{n}{2}\right) = -\mu(n)$$

and the claim follows mod 2. If $4|n$, then $\mu(n) = 0$ and every element in $\{\zeta_n^{mj}; j \in (\mathbb{Z}/n\mathbb{Z})^*\}$ appears with multiplicity (m, n) . Hence

$$2 \mid (m, n) \mid \sum_{j \in (\mathbb{Z}/n\mathbb{Z})^*} \zeta_n^{mj},$$

and we obtain the claimed congruence. \square

Proof of Lemma 3.5: Let Ξ be the set of eigenvalues of Frob_q on $H^2(\tilde{X}_{\mathbb{Q}}, \mathbb{Q}_\ell(1))$ with multiplicities. Then

$$h_q = \sum_{\zeta \in \Xi} \zeta.$$

Recall that the Galois group $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_{15}))$ acts trivially on $H^2(\tilde{X}_{\mathbb{Q}}, \mathbb{Q}_\ell(1))$. Since $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$ is Galois of degree eight, we deduce that $\zeta^8 = 1$ for each $\zeta \in \Xi$. In particular

$$(8) \quad \sum_{\zeta \in \Xi} \zeta^8 = 141.$$

In the present situation, $h_q \in \mathbb{Z}$, i.e. h_q is a sum of traces of elements in Ξ . Hence we can apply Lemma 3.12 to deduce that h_q has the same parity as the sum in (8). That is, h_q is odd. \square

4. PROOF OF THE MAIN THEOREM

There is version of the Faltings-Serre method in [Liv87] that allows to compare two-dimensional 2-adic Galois representations with even traces. Here we have to modify this approach slightly since the two-dimensional Galois representation σ_2 is only determined up to conjugation in the quadratic field F . While the original result involved the notion of non-cubic test sets, in order to prove Theorem 1.1, we replace this notion by non-quartic sets:

Definition. A subset T of a finite dimensional vector space V is *non-quartic* if every homogeneous polynomial of degree 4 on V which vanishes on T , vanishes in the whole V .

The following lemma is useful to lower the cardinality of the test set T .

Lemma 4.1. *Let V be a finite-dimensional vector space. Let T be a subset of V which contains 4 distinct hyperplanes through the origin and a point outside them. Then $T \setminus \{0\}$ is non-quartic.*

Proof. Let L_1, \dots, L_4 denote linear homogeneous polynomials giving equations of the four hyperplanes. Let $P(x_1, \dots, x_n)$ be a homogeneous quartic polynomial vanishing on all points of T . Division with remainder gives a representation

$$P(x_1, \dots, x_n) = L_1 Q(x_1, x_2, \dots, x_n) + P_2(x_1, \dots, x_n)$$

with $L_1 \nmid P_2$. The crucial property here is the following: Since T contains the hyperplane $\{L_1 = 0\}$ and P vanishes on this hyperplane, P_2 vanishes on all

of V . (To see this, apply a linear transformation so that $L_1 = x_1$; then $P_2 = P_2(x_2, \dots, x_n)$, and P_2 vanishes on the hyperplane $\{x_1 = 0\}$ if and only if it vanishes on V). Since the hyperplanes are linearly independent, we can apply the same argument to the other three hyperplanes (starting with $L_1 Q$ instead of P). We obtain

$$P(x_1, \dots, x_n) = A \cdot L_1 L_2 L_3 L_4 + \tilde{P}(x_1, \dots, x_n),$$

where A is a field constant and \tilde{P} vanishes identically on V . Since T contains a point outside the union of the four hyperplanes, A must be zero.

But then $P = \tilde{P}$ vanishes on all of V . Since this argument applies to any homogeneous quartic polynomial P , the test set $T \setminus \{0\}$ is non-quartic. \square

Remark 4.2. Note that Lemma 4.1 does explicitly not require the hyperplanes to be linearly independent. It is immediate from the proof of Lemma 4.1 that the same argument works for test sets for homogeneous polynomials of degree n if we find n distinct hyperplanes through the origin and a point outside them.

We want to compare the two Galois representations, σ_2 and $\sigma_{f,2}$. It is crucial that in the present situation we know that the Galois conjugate representation exists: this follows in the geometric example by construction, and in the modular example we can consider the 2-adic representation attached to the conjugate Hilbert modular forms f^τ , where τ is a generator of the group $\text{Gal}(F/\mathbb{Q})$. For any given ℓ -adic Galois representation ρ with field of coefficients F (i.e, the field generated by the traces of Frobenius elements is F) we will denote by ρ' the conjugate representation (if we know that such a representation exists). Since for the Calabi-Yau threefold \tilde{X} , we can only compute the traces of the 4-dimensional Galois representation $\sigma_2 \oplus \sigma'_2$ of $\text{Gal}(\overline{\mathbb{Q}}/F)$ (or actually of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$), we will need the following generalization of Theorem 4.3 in [Liv87] about Galois representations whose residual images are 2-groups:

Theorem 4.3. *Let K be a global field, S a finite set of primes of K and E the unramified quadratic extension of \mathbb{Q}_2 . Denote by K_S the compositum of all quadratic extensions of K unramified outside S and by \mathcal{P}_2 the maximal prime ideal of $\mathcal{O} := \mathcal{O}_E$. Suppose $\rho_1, \rho_2: \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GL}_2(E)$ are continuous representations, unramified outside S , and with field of coefficients F , and assume also that their Galois conjugates exist. We suppose that the following conditions are satisfied:*

1. $\text{Tr}(\rho_1) \equiv \text{Tr}(\rho_2) \equiv 0 \pmod{\mathcal{P}_2}$ and $\det(\rho_1) \equiv \det(\rho_2) \pmod{\mathcal{P}_2}$.
2. *There exists a set T of primes of K , disjoint from S , for which*
 - (i) *The image of the set $\{\text{Frob}_t\}$ in $\text{Gal}(K_S/K) \setminus \{0\}$ is non-quartic.*
 - (ii) $\text{Tr}(\rho_1(\text{Frob}_t)) + \text{Tr}(\rho'_1(\text{Frob}_t)) = \text{Tr}(\rho_2(\text{Frob}_t)) + \text{Tr}(\rho'_2(\text{Frob}_t))$ and $\det(\rho_1(\text{Frob}_t)) = \det(\rho_2(\text{Frob}_t))$ for all $t \in T$.

Then $\rho_1 \oplus \rho'_1$ and $\rho_2 \oplus \rho'_2$ have isomorphic semi-simplifications.

Proof. As in [Liv87], the Theorem follows easily from a similar statement (Proposition 4.7 in [Liv87]) where the Galois group is replaced by a pro-2 group topologically finitely generated G and the set of primes T by a subset Σ of G satisfying similar conditions. We shall now indicate how to modify the proof of Proposition 4.7 in [Liv87]. We will follow Livne's notation, so the reader should consult [Liv87] to compare with the following lines.

We define M_2 and ρ exactly as in [Liv87], but we consider M to be the \mathbb{Z}_2 -linear span of $\rho(G)$ (instead of the \mathcal{O} -span). Since \mathcal{O} has rank 2 over \mathbb{Z}_2 , M is a free module of rank at most 16 over \mathbb{Z}_2 . We consider $R = M/2M$, it is an \mathbb{F}_2 vector space of dimension at most 16. The assertion in [Liv87], page 258, generalizes to:

Assertion: R is spanned over \mathbb{F}_2 by $\{\bar{\sigma} | \sigma \in \Sigma \cup \{1\}\}$.

Let us indicate what modifications are needed to see this. Recall that now we are assuming that Σ is non-quartic.

First one has to prove the following statement:

$$(9) \quad \sigma \in \Sigma \Rightarrow \bar{\sigma}^2 = \bar{1} \text{ in } \Gamma.$$

In [Liv87], the common value of the traces for elements $\sigma \in \Sigma$ is denoted: $t = \text{Tr } \rho_1(\sigma) = \text{Tr } \rho_2(\sigma)$. Since we are not assuming that these traces are equal, we can call them instead: $t_1 = \text{Tr } \rho_1(\sigma)$, $t_2 = \text{Tr } \rho_2(\sigma)$. In his proof of the assertion the equality of traces for elements of Σ is never used. Moreover, the proof of (9) given in [Liv87] applies directly to our case because we are also in a case where G is a 2-group, thus residual traces are 0 and residual determinants are 1. The only difference is in the notation, the equality in [Liv87]:

$$\rho(\sigma)^2 = t\rho(\sigma) - d(I, I)$$

in $M_2 \times M_2$, where $\rho : G \rightarrow M_2 \times M_2$ is the map $\rho(g) = (\rho_1(g), \rho_2(g))$ now becomes:

$$\rho(\sigma)^2 = (t_1\rho_1(g), t_2\rho_2(g)) - d(I, I)$$

As in [Liv87], we see that R is a commutative ring, and also a local Artin algebra over \mathbb{F}_2 with maximal ideal

$$P = \{r \in R | r^2 = 0\}$$

and $R/P = \mathbb{F}_2$. In our case, we will show that $P^5 = 0$. The proof of this fact goes as the one given in [Liv87], except that we consider now products of 5 elements x_1, \dots, x_5 in P (instead of 4): assuming that their product is non-zero we derive a contradiction, as in [Liv87], by considering the \mathbb{F}_2 -algebra

$$R_0 = \mathbb{F}_2[T_1, \dots, T_5]/(T_1^2, \dots, T_5^2)$$

and the injective map of \mathbb{F}_2 -algebras from R_0 to R that sends T_i to x_i . The contradiction follows from the inequalities: $\dim_{\mathbb{F}_2} R_0 = 32 > 16 \geq \dim_{\mathbb{F}_2} R$.

Using the fact that $P^5 = 0$, the rest of the proof of the assertion follows as in [Liv87], changing “cubic polynomial” by “quartic polynomial”, and “non-cubic” by “non-quartic”.

Once the assertion is proved, we conclude as in [Liv87] from Nakayama's lemma that the \mathbb{Z}_2 -span of $\{\rho(\sigma) | \sigma \in \Sigma \cup \{1\}\}$ is all of M (recall that M is the linear \mathbb{Z}_2 -span of $\rho(G)$).

Here comes the only place where equality of the traces over Σ is used in Livne's proof: he considers the map: $\alpha : M \rightarrow \mathcal{O}$ defined by $\alpha(a, b) = \text{Tr } a - \text{Tr } b$. Since this map is \mathcal{O} -linear and $\alpha(I, I) = 0$, assuming that $\alpha(\rho(\sigma)) = 0$ for every $\sigma \in \Sigma$ Livne concludes that $\alpha = 0$, i.e., equality of the traces of ρ_1 and ρ_2 . We can argue in the same way but using the map: $\beta : M \rightarrow \mathbb{Z}_2$ given by

$$\beta(a, b) = \text{Tr } a + (\text{Tr } a)^\phi - \text{Tr } b - (\text{Tr } b)^\phi$$

where ϕ is the order two element in $\text{Gal}(E/\mathbb{Q}_2)$. Observe that when applied to numbers in F , ϕ agrees with the order two element τ in $\text{Gal}(F/\mathbb{Q})$.

Observe that if $a = \rho_1(g)$, then $(\text{Tr } a)^\phi = (\text{Tr } \rho_1(g))^\phi = \text{Tr}(\rho'_1(g))$, and similarly for $b = \rho_2(g)$. This map is \mathbb{Z}_2 -linear and satisfies $\beta(I, I) = 0$. Then, assumption (2) (ii) in the theorem implies that for elements of G in Σ (these elements correspond to Frobenius elements for primes in T) the map β vanishes, thus we conclude (as Livne does for α) that $\beta = 0$, which is the equality of the traces of two 4-dimensional 2-adic Galois representations. Applying Brauer-Nesbitt we conclude that these 4-dimensional Galois representations have isomorphic semi-simplifications. \square

Proof of Theorem 1.1. We want to apply Theorem 4.3 to the 2-adic Galois representations $\sigma_2, \sigma_{f,2}$ over $F = K$. In Proposition 3.3 we proved that σ_2 has even traces by geometric considerations, and in Section 2 we proved that the same is true for the representation $\sigma_{f,2}$. Recall from the introduction that both residual representations $\bar{\sigma}_2, \bar{\sigma}_{f,2}$ have image in $\text{SL}(\mathbb{F}_4)$. In particular their determinants are congruent modulo 2. Thus the first hypothesis of Theorem 4.3 is satisfied. The field K_S of Theorem 4.3 is the compositum of the thirty one field extensions computed in the proof of Proposition 2.9. The set of primes in K in the set

$$\begin{aligned} T = \{ & \langle 61, 26 - \sqrt{5} \rangle, \langle 59, \sqrt{5} + 8 \rangle, \langle 149, \sqrt{5} - 68 \rangle, \langle 211, \sqrt{5} + 65 \rangle, \langle 101, \sqrt{5} - 45 \rangle, \\ & \langle 19, \sqrt{5} + 9 \rangle, \langle 229, \sqrt{5} - 66 \rangle, \langle 11, \sqrt{5} - 4 \rangle, \langle 11, \sqrt{5} + 4 \rangle, \langle 109, \sqrt{5} - 21 \rangle, \\ & \langle 19, \sqrt{5} - 9 \rangle, \langle 701, \sqrt{5} - 53 \rangle, \langle 211, \sqrt{5} - 65 \rangle, \langle 29, \sqrt{5} - 11 \rangle, \langle 59, \sqrt{5} - 8 \rangle, \\ & \langle 181, \sqrt{5} - 27 \rangle, \langle 239, \sqrt{5} + 31 \rangle, \langle 31, \sqrt{5} + 6 \rangle, \langle 79, \sqrt{5} - 20 \rangle, \langle 71, \sqrt{5} - 17 \rangle, 13, \\ & \langle 401, \sqrt{5} - 178 \rangle, \langle 449, \sqrt{5} - 118 \rangle, \langle 241, \sqrt{5} - 103 \rangle, \langle 89, \sqrt{5} - 19 \rangle, 7, \\ & \langle 79, \sqrt{5} + 20 \rangle, \langle 239, \sqrt{5} - 31 \rangle, \langle 41, \sqrt{5} - 13 \rangle, \langle 31, \sqrt{5} - 6 \rangle, \langle 71, \sqrt{5} + 17 \rangle \}, \end{aligned}$$

saturate the set $\text{Gal}(K_S/K) \setminus \{0\}$. They are ordered in such a way that the primes (under class field theory) correspond to the extensions listed in Table 2.1 in the same order.

Thus T saturates the set $\text{Gal}(K_S/K) \setminus \{0\}$, but we can still eliminate some prime ideals of big norm by replacing T by a non-quartic test set by Lemma 4.1. To do so, we fix a standard basis of \mathbb{F}_2^5 corresponding to the following quadratic extensions of F :

$$x^2 - 3\frac{\sqrt{5}-5}{2}, x^2 - 3, x^2 + \frac{\sqrt{5}+5}{2}, x^2 - 3\sqrt{5}, x^2 - 2.$$

In this basis, the elements corresponding to the primes above 701, 449 and 401 correspond to the elements $(1, 1, 0, 0, 1)$, $(0, 1, 1, 1, 0)$ and $(1, 1, 0, 1, 0)$ respectively in \mathbb{F}_2^5 .

We claim that the set T' obtained from T by removing these three elements is a non-quartic set in \mathbb{F}_2^5 . To see this, we use Lemma 4.1 with the fact that $T' \cup \{0\}$ contains the four hyperplanes

$$\begin{cases} x_2 = 0 \\ x_4 + x_5 = 0 \\ x_1 + x_3 = 0 \\ x_1 + x_2 + x_3 + x_4 + x_5 = 0 \end{cases}$$

and the extra point $(0, 1, 1, 0, 1)$ (which corresponds to one of the primes above 59).

It was checked in [CS01] that the characteristic polynomials of the 4-dimensional Galois representations $\sigma_2 \oplus \sigma'_2$ and $\sigma_{f,2} \oplus \sigma_{f^r,2}$ agree at the primes of K above rational primes smaller than 100. For the remaining set of primes above the set of rational primes

$$\{101, 109, 149, 181, 211, 229, 239, 241\},$$

the same was checked by us, see Appendix A and the table at [DPS]. By Theorem 4.3 we conclude that the two 4-dimensional Galois representations have indeed isomorphic semi-simplifications. In particular, any irreducible component of one of them must be isomorphic to some irreducible component of the other, thus since we know that $\sigma_{f,2}$ and $\sigma_{f^r,2}$ are irreducible, one of them must be isomorphic to σ_2 (and the other to σ'_2). This proves Theorem 1.1. \square

APPENDIX A. COUNTING POINTS

In this appendix we indicate how to count the number of points on the Consani-Scholten quintic \tilde{X} over finite fields. In particular, we give the traces of the Galois representations $\sigma_\lambda, \sigma'_\lambda$ at the primes $p > 100$ needed to prove Theorem 1.1. For most part, we follow the approach from [CS01].

Recall that \tilde{X} is given affinely by the symmetric equation in the Chebyshev polynomial $P_5(y, z)$:

$$X = \{P_5(x_1, x_2) = P_5(x_4, x_5)\} \subset \mathbb{A}^4.$$

Thus we can count the number of points of \tilde{X} over some finite field \mathbb{F}_q as follows:

- (1) Compute the affine number of points $\#X(\mathbb{F}_q)$.

- (2) For the projective closure $\bar{X} \subset \mathbb{P}^4$, let $S \subset \mathbb{P}^3$ be $\bar{X} - X$. Compute $\#S(\mathbb{F}_q)$.
- (3) Compute the contribution from the exceptional divisors in the resolution $\tilde{X} \rightarrow \bar{X}$.

For (1), we can proceed by counting how often each value in \mathbb{F}_q is attained by the Chebyshev polynomial $P_5(y, z)$ over \mathbb{A}^2 . Due to the symmetry, $\#X(\mathbb{F}_q)$ is the sum of the squares of these numbers.

For (2), note that S is the Fermat quintic given by the model

$$S = \{x_1^5 + x_2^5 = x_4^5 + x_5^5\} \subset \mathbb{P}^3.$$

In [CS01] it was pointed out that for $q \not\equiv 1 \pmod{5}$ one has $\#S(\mathbb{F}_q) = 1 + q + q^2$. Meanwhile for $q \equiv 1 \pmod{5}$, we could either use the zeta function of S and its description in terms of Jacobi symbols due to A. Weil or proceed along the same lines as above, i.e. count points over \mathbb{A}^4 using symmetry and then take into account that we are actually working over \mathbb{P}^3 (subtract 1 and divide by $q-1$). However either approach would a priori impose the same complexity as for computing $\#X(\mathbb{F}_q)$. Luckily counting $\{(y, z) \in \mathbb{A}_{\mathbb{F}_q}^2; y^5 + z^5 = a\}$ can be improved by noting that scalar multiplication acts as multiplication by fifth powers on the values. Hence $\#\{(y, z) \in \mathbb{A}_{\mathbb{F}_q}^2; y^5 + z^5 = 0\} = (q-1) \cdot \#\{[y, z] \in \mathbb{P}_{\mathbb{F}_q}^1; y^5 + z^5 = 0\} + 1$ and for any $a \neq 0$ with $O(a) = a \cdot (\mathbb{F}_q^*)^5$ denoting the a -orbit under multiplication by fifth powers in \mathbb{F}_q^* :

$$\#\{(y, z) \in \mathbb{A}_{\mathbb{F}_q}^2; y^5 + z^5 = a\} = 5 \sum_{o \in O(a)} \#\{[y, z] \in \mathbb{P}_{\mathbb{F}_q}^1; y^5 + z^5 = o\}.$$

(Strictly speaking the sets on the right are ambiguous, but scalar multiples end up in the same orbit, so the contribution does not depend on the chosen representative $[y, z] \in \mathbb{P}^1$.) Essentially this simplification reduces the algorithm's running time from q^2 to q compared with computing $\#X(\mathbb{F}_q)$.

Finally for (3) we recall from 3.3 that the 120 nodes are always defined over the extension of \mathbb{F}_q containing the 15th roots of unity, and that their rulings are always defined over the same field. So if a node is defined over \mathbb{F}_q , then its exceptional divisor contributes $q^2 + 2q$ additional points.

Thus we find $\#\tilde{X}(\mathbb{F}_q)$. This allows us to compute the trace

$$a_q = \text{trace } \text{Frob}_q^*(H^3(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell))$$

through the Lefschetz fixed point formula (2). Here we do not need to know h_q in advance since it is determined (for $q > 20$ and $b_3(\tilde{X}) = 4$) by the inequality

$$|a_q| \leq 4q^{3/2}.$$

We obtain the characteristic polynomial of Frob_q^* on $H^3(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$:

$$L_q(T) = T^4 - a_q T^3 + \frac{1}{2}(a_q^2 - a_{q^2})T^2 - a_q q^3 T + q^6.$$

In the present situation, we know that $L_q(T)$ will always split over $\mathbb{Q}(\sqrt{5})$:

$$L_q(T) = (T^2 - \alpha_q T + q^3)(T^2 - \alpha_q^\sigma T + q^3), \quad \alpha \in \mathbb{Q}(\sqrt{5}).$$

The traces $\alpha_p, \alpha_p^\sigma$ appear as coefficients of the Hilbert modular form. In the following table, we collect one of the traces together with the numbers of points of X and S over \mathbb{F}_p and \mathbb{F}_{p^2} for all primes $p > 100$ needed to prove Theorem 1.1.

p	$\#X(\mathbb{F}_p)$	$\#X(\mathbb{F}_{p^2})$	$\#S(\mathbb{F}_p)$	$\#S(\mathbb{F}_{p^2})$	α_p
101	1222681	1063601210405	14655	104338955	$-598 - 476\sqrt{5}$
109	1338593	1679922873825	11991	141787855	$890 + 468\sqrt{5}$
149	3395857	10952392903505	22351	494061055	$150 - 344\sqrt{5}$
181	6562145	35183310464645	39455	1074841355	$-898 - 288\sqrt{5}$
211	10261235	88285583898085	49205	1984280555	$-1228 - 1616\sqrt{5}$
229	12214593	144270849112465	52671	2752837855	$-210 + 940\sqrt{5}$
239	13872967	186440164574105	57361	3265836055	$3240 + 944\sqrt{5}$
241	15137985	195998061709305	65255	3375066455	$-4938 + 172\sqrt{5}$

APPENDIX B. STURM BOUND (BY JOSÉ BURGOS GIL AND ARIEL PACETTI)

The aim of this appendix is to show how a Sturm bound can be obtained for the modular form of level $6\sqrt{5}$ and weight $(2, 4)$. We expect to extend the result to any real quadratic fields in a future work. Following the previous notation, F will denote the real quadratic field $\mathbb{Q}[\sqrt{5}]$.

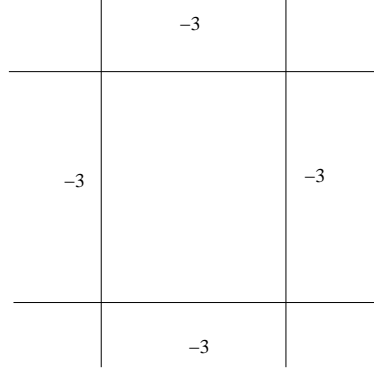
B.1. Desingularization and a Sturm bound over \mathbb{C} . Let $H(3)$ be the Hilbert modular surface obtained as the quotient of the product of two copies of the Poincaré upper half plane modulo the action of the congruence group

$$\Gamma(3) := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_F) : \alpha \equiv \delta \equiv 1 \pmod{3}, \beta, \gamma \in 3\mathcal{O}_F \right\}.$$

The group $\Gamma(3)$ has no fixed elliptic points for this action (see [vdG88] page 109); it has 10 non-equivalent cusps. Let $\overline{H}(3)$ be the minimal compactification of $H(3)$ obtained by adding one point for each cusp. The surface $\overline{H}(3)$ is singular at all such points. Denoting by $\tilde{H}(3)$ the minimal desingularization of $\overline{H}(3)$, we get that the diagram of the desingularization of $\overline{H}(3)$ at any cusp is the following (see [vdG88], page 193):

Denote by c_i , $1 \leq i \leq 10$ the different cusps (where c_1 is the cusp at infinity) and denote by S_i , $1 \leq i \leq 10$ the exceptional divisor at the i -th cusp. The surface $\tilde{H}(3)$ is of general type (by Theorem 3.4 of [vdG88]).

We want a criterion to show that a Hilbert modular form whose Fourier expansion starts with many zeroes is actually the zero modular form. This is a



generalization of the Sturm bound to Hilbert modular forms. To this end we need a nef (numerically eventually free) divisor. Let F_1 be the curve defined in [vdG88] page 88. It has 30 disjoint connected components made of curves with self-intersection number -2 and it meets each connected component of the desingularization at the cusps in three points (see [vdG88], page 193).

Lemma B.1. *The intersection numbers between the curves S_i and F_1 are:*

- $S_i \cdot S_j = \begin{cases} 0 & \text{if } i \neq j, \\ -4 & \text{if } i = j. \end{cases}$
- $F_1 \cdot F_1 = -60.$
- $S_i \cdot F_1 = 12.$

Consider the divisor

$$D' := \frac{1}{5} \left(\sum_{i=1}^{10} S_i + 2F_1 \right).$$

Lemma B.2. *The divisor D' is nef and it agrees with the canonical divisor. Its self-intersection number is given by*

$$D' \cdot D' = 8.$$

Proof. In example 7.5 of [vdG88] (page 179) it is proved that D' equals the canonical divisor and its self-intersection number is computed. The fact that it is nef follows from the fact that $\tilde{H}(3)$ is a minimal surface of general type. \square

Let $M_{2k}(\Gamma(3))$ denote the vector space of modular forms of parallel weight $2k$ for $\Gamma(3)$. It is the space of global sections of the line bundle $\mathcal{O}(k(D' + S)) = \mathcal{O}(D' + S)^{\otimes k}$:

$$M_{2k}(\Gamma(3)) = \Gamma(\mathcal{O}(k(D' + S))),$$

where $S = \sum_{i=1}^{10} S_i$. Similarly, the space of cusp forms $S_{2k}(\Gamma(3))$ is given by the divisor $k(D' + S) - S$.

We want to add some vanishing conditions to $M_{2k}(\Gamma(3))$ such that the space of forms with these vanishing conditions is empty. Let a be a positive integer,

and G be a Hilbert modular form. We say that G vanishes with order a at the cusp c_i if G is a section of $\mathcal{O}(k(D' + S) - aS_i) \subset \mathcal{O}(k(D' + S))$.

Let G be a form which vanishes with order a at all the cusps and with order $a + b$ at the infinity cusp, i.e. it belongs to the space given by the divisor

$$E = k(D' + S) - aS - bS_1.$$

It follows from Lemma B.1 and Lemma B.2 that $D' \cdot S_i = 4$ for all $1 \leq i \leq 10$, so

$$E \cdot D' = k(D' \cdot D' + S \cdot D') - aS \cdot D' - bS_1 \cdot D' = 48k - 40a - 4b.$$

If $b + 10a > 12k$, this intersection number is negative and, since D' is nef, the space of global sections of $\mathcal{O}(E)$ is the zero space. This implies

Theorem B.3. *If G is a Hilbert modular form of parallel weight $2k$ for $\Gamma(3)$ which vanishes with order a at all cusps and with order $a + b$ at the infinity cusp and $b + 10a > 12k$, then G is the zero form.*

Corollary B.4. *If G is a Hilbert modular form of weight (k_1, k_2) , with $k_1 \equiv k_2 \pmod{2}$, for $\Gamma(3)$ which vanishes with order a at all cusps and with order $a + b$ at the infinity cusp and $b + 10a > 3(k_1 + k_2)$, then G is the zero form.*

Proof. Just apply the previous Theorem to the form $G(z_1, z_2) \cdot G(z_2, z_1)$. \square

To relate the order of vanishing of a modular form at a cusp with the q -expansion we need to compute explicitly the first step of the desingularization of the cusp. In the case of the infinity cusp, this implies computing the local ring of the cusp, which is done in [vdG88] Chapter II, Section 2. The stabilizer of the infinity cusp for $\Gamma(3)$ is given by

$$\left\{ \begin{pmatrix} \epsilon & \alpha \\ 0 & \epsilon^{-1} \end{pmatrix} : \alpha \in 3\mathcal{O}_F \text{ and } \epsilon \equiv 1 \pmod{3} \right\},$$

i.e. it is of type $(M, V) = (3\mathcal{O}_F, U_F^8)$, where $U_F^8 = \langle \frac{47}{2} + \frac{3}{2}\sqrt{5} \rangle$. The dual of M is given by $M^\vee = \frac{\mathcal{O}_F^\vee}{3} = \frac{\mathcal{O}_F}{3\sqrt{5}}$, so any Hilbert modular form for $\Gamma(3)$ has a q -expansion at the infinity cusp of the form

$$\sum_{\substack{\xi \gg 0 \\ \xi \in \frac{\mathcal{O}_F}{3\sqrt{5}}}} a_\xi \exp(\xi z_1 + \tau(\xi) z_2).$$

Let M_+ denote the elements of M which are totally positive, and consider the embedding of M_+ in $(\mathbb{R}_+)^2$, given by

$$\mu \mapsto (\mu, \tau\mu).$$

Denote by $A_k = (A_k^1, A_k^2)$, $k \in \mathbb{Z}$ the vertices of the boundary of the convex hull of the image of M_+ , ordered with the condition $A_{k+1}^1 < A_k^1$ for all k . Any

pair (A_{k-1}, A_k) is a basis for M as \mathbb{Z} -module (see [vdG88] Lemma 2.1). This determines an isomorphism

$$M \setminus \mathbb{C}^2 \mapsto \mathbb{C}^\times \times \mathbb{C}^\times,$$

which maps $z = (z_1, z_2)$ to (u_{k-1}, u_k) , where

$$(10) \quad \exp(z_j) = u_{k-1}^{A_{k-1}^j} u_k^{A_k^j}, \quad \text{for } j = 1, 2.$$

Let σ_k denote the cone spanned by A_{k-1} and A_k , i.e.

$$\sigma_k = \{sA_{k-1} + tA_k : s, t \in \mathbb{R}_+\}.$$

The desingularization of the infinity cusp is obtained by taking a copy of \mathbb{C}^2 for each element σ_k and gluing them together in terms of the change of basis matrix (see [vdG88] page 31).

Let $\xi \in M^\vee$ be a totally positive element. Then in the copy corresponding to σ_k ,

$$\begin{aligned} \exp(\text{Tr}(\xi z)) &= \exp(\xi z_1 + \tau(\xi) z_2) = u_{k-1}^{\xi A_{k-1}^1 + \tau(\xi) A_{k-1}^2} \cdot u_k^{\xi A_k^1 + \tau(\xi) A_k^2} = \\ &= u_{k-1}^{\text{Tr}(\xi A_{k-1})} \cdot u_k^{\text{Tr}(\xi A_k)}. \end{aligned}$$

Now, we denote by L_k , the component of the exceptional divisor S_1 , over the infinity cusp, that corresponds to the ray through A_k . Observe that $L_{k+4} = L_k$. We have:

Proposition B.5. *Let G be a Hilbert modular form with q -expansion at infinity*

$$G(z_1, z_2) = \sum_{\substack{\xi \gg 0 \\ \xi \in \frac{0}{3\sqrt{5}}F}} a_\xi \exp(\xi z_1 + \tau(\xi) z_2).$$

Let L_k be as above. Then $\text{ord}_{L_k}(G) > K$ if and only if $a_\xi = 0$ for all $\xi \in M^\vee$, $\xi \gg 0$ with $\text{Tr}(\xi A_k) \leq K$.

Name	Point
A_0	$3(1, 1)$
A_1	$3(1 + \omega, 1 + \tau(\omega))$
A_2	$3(2 + 3\omega, 2 + 3\tau(\omega))$
A_3	$3(5 + 8\omega, 5 + 8\tau(\omega))$

TABLE B.1. First boundary points

In Table B.1 it is shown a set of nonequivalent boundary points of the convex hull of M_+ , where ω denotes the element $\frac{1+\sqrt{5}}{2}$. It is clear that they differ by powers of ω^2 , and since the matrix $\begin{pmatrix} \omega^2 & 0 \\ 0 & \omega^{-2} \end{pmatrix} \in \Gamma_0(3)$, a Hilbert modular form for

$\Gamma_0(3)$ will vanish with the same order in the four components L_k , $k = 0, \dots, 3$, of S_1 . The vanishing condition corresponding to L_0 , reads

$$\text{ord}_{L_0}(\exp(\xi z)) = 3 \text{Tr}(\xi).$$

In particular, a modular form vanishes at the cusp if and only if $a_0 = 0$.

The above discussion implies

Theorem B.6. *Let G be a Hilbert modular form of parallel weight $2k$ for $\Gamma_0(3)$ which vanishes with order a at all cusps and whose Fourier expansion at the infinity cusp is given by*

$$G = \sum_{\substack{\xi \gg 0 \\ \xi \in \frac{\mathcal{O}_F}{3\sqrt{5}}}} a_\xi \exp(\xi z_1 + \tau(\xi) z_2).$$

If $a_\xi = 0$ for all ξ with $\text{Tr}(\xi) \leq 4k - 3a$ then G is the zero form.

Proof. If $a_\xi = 0$ for all ξ with $\text{Tr}(\xi) \leq 4k - 3a$, by Proposition B.5, G vanishes with order greater than $12k - 9a$ at the infinity cusp. Thus the result follows from Theorem B.3. \square

Corollary B.7. *Let G be a Hilbert modular form of weight (k_1, k_2) , with $k_1 \equiv k_2 \pmod{2}$, for $\Gamma_0(3)$ which vanishes with order a at all cusps and whose Fourier expansion at the infinity cusp is given by*

$$G = \sum_{\substack{\xi \gg 0 \\ \xi \in \frac{\mathcal{O}_F}{3\sqrt{5}}}} a_\xi \exp(\xi z_1 + \tau(\xi) z_2).$$

If $a_\xi = 0$ for all ξ with $\text{Tr}(\xi) \leq (k_1 + k_2) - 3a$ then G is the zero form.

B.2. Moduli interpretation and integral models. In order to make the computation of the previous section work over finite fields, we need to use the integral structure of the modular Hilbert surface and of the modular curve $X(3)$. It comes from their moduli interpretation. Let us follow the notation of [BBGK07].

We fix ζ_3 a third-root of unity and we denote by $\delta = (\sqrt{5})^{-1}$ the different of F .

An abelian scheme $A \rightarrow S$ of relative dimension 2, together with a ring homomorphism

$$\iota : \mathcal{O}_F \rightarrow \text{End}(A)$$

is called an abelian surface with multiplication by \mathcal{O}_F , and is denoted by the pair (A, ι) . This gives an \mathcal{O}_F -multiplication in the dual abelian surface A^\vee . An element $\mu \in \text{Hom}(A, A^\vee)$ is called \mathcal{O}_F -linear if $\mu\iota(\alpha) = \iota(\alpha)^\vee \mu$ for all $\alpha \in \mathcal{O}_F$. Denote by $\mathcal{P}(A)$ the sheaf for the $i_{\mathcal{L}}^{\frac{1}{2}}$ -tale topology on Sch/S defined by

$$\mathcal{P}(A)_T = \{\lambda : A_T \rightarrow A_T^\vee : \lambda \text{ is symmetric and } \mathcal{O}_F\text{-linear}\},$$

for all $T \rightarrow S$. The subsheaf $\mathcal{P}(A)^+$ is the subsheaf of polarizations in $\mathcal{P}(A)$. The pair (A, ι) is said to satisfy the Deligne-Pappas condition, denoted by (DP), if the canonical morphism of sheaves

$$A \otimes_{\mathcal{O}_F} \mathcal{P}(A) \mapsto A^\vee$$

is an isomorphism. In this case, $\mathcal{P}(A)$ is a locally constant sheaf of projective \mathcal{O}_F -modules of rank 1.

Since the class number of \mathcal{O}_F is one, we can restrict to consider only \mathcal{O}_F -polarizations. An \mathcal{O}_F -polarization on a pair (A, ι) is a morphism of \mathcal{O}_F -modules $\psi : \mathcal{O}_F \rightarrow \mathcal{P}(A)_S$ taking \mathcal{O}_F^+ to $\mathcal{P}(A)^+$ such that the natural homomorphism

$$A \otimes_{\mathcal{O}_F} \mathcal{O}_F \rightarrow A^\vee, \quad a \otimes \alpha \mapsto \psi(\alpha)(a)$$

is an isomorphism.

Suppose S is a scheme over $\text{Spec } \mathbb{Z}[1/3]$. A level 3-structure on an abelian surface A over S with real multiplication by \mathcal{O}_F is an \mathcal{O}_F -linear isomorphism

$$\varphi : (\mathcal{O}_F/3)^2_S \rightarrow A[3]$$

between the constant group scheme defined by $(\mathcal{O}_F/3)^2$ and the 3-torsion of A .

Theorem B.8. *The moduli problem “Abelian surfaces over S with real multiplication by \mathcal{O}_F satisfying (DP) condition, \mathcal{O}_F -polarization and level 3-structure” is represented by a regular algebraic scheme $\mathcal{H}(3)$ which is flat and of relative dimension two over $\text{Spec } \mathbb{Z}[1/3, \xi_3]$. Furthermore, it is smooth over $\text{Spec } \mathbb{Z}[1/15, \xi_3]$.*

Proof. See [Gor02] Theorem 2.17, p. 57; Lemma 5.5, p. 99. \square

Remark B.9. The scheme $\mathcal{H}(3)$ is not geometrically irreducible, it has $\#(\mathcal{O}_F/3)^\times = 8$ connected components over $\bar{\mathbb{Q}}$. In fact, the 8 components are defined over $\text{Spec } \mathbb{Z}[1/15, \xi_3]$. This definition is not the same as the one given in [Rap78], it is a topological cover of degree 4 of it. Let S be a scheme over $\mathbb{Z}[1/3]$, then the abelian scheme A has a Weil pairing $e_3 : A[3] \times A^\vee[3] \mapsto \mu_3$, which satisfies $e_3(\alpha a, b) = e_3(a, \alpha b)$. There exists an \mathcal{O}_F -bilinear form $e_{\mathcal{O}_F} : A[3] \times A^\vee[3] \mapsto (\delta^{-1}/3\delta^{-1})(1)$ such that $e_3 = \text{Tr}(e_{\mathcal{O}_F})$. Any element in $\lambda \in \mathcal{P}(A)_T$ defines a homomorphism between A and A^\vee which is trivial on $A[3]$ if and only if $\lambda \in 3\mathcal{P}(A)_T$ for any morphism $T \rightarrow S$. Since $e_{\mathcal{O}_F}$ is non-degenerate, $\mathcal{P}(A) \otimes_{\mathcal{O}_F} \Lambda_{\mathcal{O}_F}^2 A[3] = \delta^{-1}/3\delta^{-1}(1)$.

Any element $\phi \in \text{Isom}(\mu_3, \mathbb{Z}/3)$ gives an isomorphism between $\delta^{-1}/3\delta^{-1}(1)$ and $\delta^{-1}/3\delta^{-1}$. In [Rap78] the only level 3-structures considered are the φ such that in the following diagram

$$\begin{array}{ccc} \mathcal{P}(A) \otimes_{\mathcal{O}_F} \Lambda_{\mathcal{O}_F}^2 A[3] & \xlongequal{\quad} & \delta^{-1}/3\delta^{-1}(1) \\ \downarrow e_{\mathcal{O}_F} \otimes \psi \sim & & \vdots \\ \delta^{-1} \otimes_{\mathcal{O}_F} \Lambda_{\mathcal{O}_F}^2 (\mathcal{O}_F/3) & \xlongequal{\quad} & \delta^{-1}/3\delta^{-1} \end{array}$$

the vertical dotted arrow is given by an element $\phi \in \text{Isom}(\mu_3, \mathbb{Z}/3)$. Since all such maps differ by (multiplication by) an element in $(\mathcal{O}_F/3)^\times$, the two assertions follow.

Remark B.10. The advantage of the moduli problem considered in [Rap78] is that it is geometrically connected over \mathbb{Q} , and the 2-connected components over $\bar{\mathbb{Q}}$ are Galois conjugate of each other.

Remark B.11. The group $\text{GL}_2(\mathcal{O}_F/3)$ acts on $\mathcal{H}(3)$, where an element M send a level 3-structure φ to the level 3-structure $\varphi \circ M$. The subgroup $\text{SL}_2(\mathcal{O}_F/3)$ acts on each connected component of $\mathcal{H}(3) \otimes \bar{\mathbb{Q}}$, while the subgroup $H_F = \{ \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \text{ such that } \alpha \in (\mathcal{O}_F/3)^\times \}$ acts transitively on the set of connected components.

Theorem B.12. *There is a toroidal compactification $h_3: \widetilde{\mathcal{H}}(3) \mapsto \mathbb{Z}[\zeta_3, 1/3]$ of $\mathcal{H}(3)$ that is smooth at infinity. The complement $\widetilde{\mathcal{H}}(3) \setminus \mathcal{H}(3)$ is a relative divisor with normal crossings.*

Proof. See [Cha90] Theorem 3.6, Theorem 4.3 and [Rap78] Theorem 5.1 and Theorem 6.7. \square

The set of complex points of $\mathcal{H}(3)$ is equal to 8 copies of the surface $H(3)$ considered in the previous section, while the set of complex points of $\widetilde{\mathcal{H}}(3)$ is equal to 8 copies of $\widetilde{H}(3)$.

If we study the moduli problem for 1-dimensional abelian varieties (i.e. elliptic curves), we have the advantage that they are already principally polarized. As in the two-dimensional case, if S is a scheme over $\mathbb{Z}[1/3]$, a level 3-structure on an elliptic curve E over S is a \mathbb{Z} -linear isomorphism

$$\varphi: (\mathbb{Z}/3)_S^2 \rightarrow E[3]$$

between the constant group scheme defined by $(\mathbb{Z}/3)^2$ and the 3-torsion of E .

Theorem B.13. *The moduli problem “elliptic curves over S with level 3-structure” is represented by a smooth affine curve $\mathcal{Y}(3)$ over $\mathbb{Z}[1/3]$. Furthermore, the category $\mathcal{M}_3[1/3]$ of “generalized elliptic curves over S , that have smooth generic fibres, singular fibres whose Neron polygons have 3-sides and with a level 3-structure” is a projective smooth scheme $\mathcal{X}(3)$ over $\mathbb{Z}[1/3]$.*

Proof. See [DR73], Corollary 2.9. \square

Remark B.14. The group $\text{GL}_2(\mathbb{Z}/3)$ acts on $\mathcal{X}(3)$, in the same way as in the two dimensional case, i.e. an element $M \in \text{GL}_2(\mathbb{Z}/3)$ sends the level 3-structure φ to the level 3-structure $\varphi \circ M$. The subgroup $\text{SL}_2(\mathbb{Z}/3)$ acts on each connected component of $\mathcal{X}(3) \otimes \bar{\mathbb{Q}}$ while the subgroup $H_{\mathbb{Q}} = \{ \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \text{ such that } \alpha \in (\mathbb{Z}/3)^\times \}$ acts transitively in the set of connected components.

We want to study the inclusions of $\mathcal{Y}(3)$ into $\mathcal{H}(3)$. If E is an elliptic curve over S , the abelian variety $A_E = E \otimes_{\mathbb{Z}} \mathcal{O}_F$ has a canonical \mathcal{O}_F -action $\iota_E: \mathcal{O}_F \rightarrow \text{End}(A_E)$. Furthermore,

$$A_E \simeq E \times_S E,$$

where the isomorphism depends on choosing a basis for \mathcal{O}_F as \mathbb{Z} -module. The dual abelian variety A_E^\vee is isomorphic to $E \otimes_{\mathbb{Z}} \delta^{-1}$. Furthermore, $\mathcal{P}(A_E) \simeq \delta^{-1} \simeq \mathcal{O}_F$ (i.e. A_E has a canonical principal polarization ψ_E), where the isomorphism preserves positivity and the Deligne-Pappas condition holds (see [BBGK07] Lemma 5.10). Let (E, φ) be an elliptic curve with level 3-structure.

Consider the natural inclusion $\text{SL}_2(\mathbb{Z}/3) \hookrightarrow \text{SL}_2(\mathcal{O}_F/3)$, and let $\mathcal{N} = \{N_i\}_{i=1}^{30}$ be a set of representatives for the quotient set $\text{SL}_2(\mathcal{O}_F/3)/\text{SL}_2(\mathbb{Z}/3)$. Each element N of \mathcal{N} gives rise to an embedding of $\mathcal{Y}(3)$ into $\mathcal{H}(3)$, which associates to the pair (E, φ) the element $(A_E, \iota_E, \psi_E, \varphi \circ N)$. For shortness we abuse notation by writing $\varphi \circ N$. The map φ extends by \mathcal{O}_F -linearity to a map

$$\tilde{\varphi}: (\mathbb{Z}/3)^2 \otimes_{\mathbb{Z}} \mathcal{O}_F = (\mathcal{O}_F/3)^2 \rightarrow A_E[3],$$

and the element N acts in $(\mathcal{O}_F/3)^2$. By choosing a connected component of $\mathcal{Y}(3) \otimes \bar{\mathbb{Q}}$ and of $\mathcal{H} \otimes \bar{\mathbb{Q}}$, the 30 embeddings obtained from the set \mathcal{N} (up to composition with an element of H_F if necessary) give us open dense subsets of the 30 connected components of the curve F_1 from the previous section.

Theorem B.15. *The closed immersion $\mathcal{Y}(3) \hookrightarrow \mathcal{H}(3)$ of schemes over $\mathbb{Z}[\zeta_3, 1/15]$ extends to a closed immersion $\mathcal{X}(3) \hookrightarrow \mathcal{H}(3)$.*

Proof. It is enough to consider the diagonal embedding, since all the other ones differ from this one by the action of the elements in \mathcal{N} .

We know that $\mathcal{X}(3) \setminus \mathcal{Y}(3)$ is a relative divisor with one component for each cusp of $X(3)$. We fix one cusp $c \in X(3)$. We want to show that the diagonal morphism can be extended to the horizontal divisor defined by c that we denote by \bar{c} . Let g be a modular form on $X(3)$ with integral coefficients, such that $g(c) = 1$, and that vanishes on all the other cusps. By the q -expansion principle, g is a modular form on $\mathcal{X}(3)$. Moreover, $\mathcal{U} = \mathcal{X}(3) \setminus \text{div}(g)$ is an affine scheme, that is an open neighborhood of \bar{c} . Moreover, shrinking \mathcal{U} if necessary, we may assume that, in addition, the ideal of \bar{c} on \mathcal{U} is principal, generated by a function f . Let $A = \Gamma(\mathcal{U}, \mathcal{O}_{\mathcal{U}})$. Then A is an integral Noetherian domain.

Thus, we need to show that the map $\mathcal{U} \setminus \bar{c} \rightarrow \mathcal{H}(3)$ can be extended to a map $\mathcal{U} \rightarrow \widetilde{\mathcal{H}}(3)$. To this end we will use the following lemma.

Lemma B.16. *Let A be an integral domain and $f \in A$ not a unit. Denote by $A_f = A[f^{-1}]$ the localization with respect to f and by $\hat{A}_{(f)}$ the completion with respect to the ideal (f) . Let X be a scheme. If $\varphi_0: \text{Spec}(A_f) \rightarrow X$ and $\hat{\varphi}: \text{Spec}(\hat{A}_{(f)}) \rightarrow X$ are morphisms of schemes that agree when restricted to $\text{Spec}((\hat{A}_{(f)})_f)$, then they glue together to give a map $\varphi: \text{Spec}(A) \rightarrow X$.*

Proof. We could just invoke fpqc descent [SGA03] (Exposé VIII), but in this case, it is even simpler to prove the lemma by hand than to check the hypothesis of fpqc descent. First it is clear, by gluing morphisms of schemes, that we can reduce to the case when $X = \operatorname{Spec}(B)$ is an affine scheme. The hypothesis assure us that, in the commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & \widehat{A}_{(f)} \\ \downarrow & & \downarrow \\ A_f & \longrightarrow & (\widehat{A}_{(f)})_f, \end{array}$$

all arrows are injective. Hence the statement is equivalent to prove that $A = \widehat{A}_{(f)} \cap A_f$. Let $b \in \widehat{A}_{(f)} \cap A_f$. Since it belongs to $\widehat{A}_{(f)}$, b is represented by a family $\{(a)_n\}_{n \in \mathbb{N}}$, where $a_n \in A/(f)^n$, satisfying the obvious compatibility relations. Since b belongs to A_f , it is represented by a quotient a/f^i , for some $a \in A$ and $i \geq 0$. By the injectivity of the maps above, the fact that $\{(a)_n\}_{n \in \mathbb{N}} = a/f^i$ in $(\widehat{A}_{(f)})_f$ implies that $[a]_n = f^i a_n$, where $[a]_n$ denotes the class of a in $A/(f)^n$. Therefore $[a]_i = 0$, so a is divisible by f^i and $a/f^i \in A$. \square

Let u_0, u_1 be the coordinates given in equation (10) corresponding to vertices A_0 and A_1 of table B.1. Denote $\widehat{B} = \mathbb{Z}[\zeta_3, \frac{1}{15}][u_0, u_1][u_0 \cdot u_1]$. According to [Rap78] Theorem 5.1, there is a morphism of schemes $\operatorname{Spec}(\widehat{B}) \rightarrow \widetilde{\mathcal{H}}(3)$.

By the q -expansion principle for the modular curve, $\widehat{A}_{(f)} = \mathbb{Z}[\zeta_3, \frac{1}{15}][q]$. By the q -expansion principle for the Hilbert modular surface, any form in $\widetilde{\mathcal{H}}(3)$ has an expansion of the form $\sum_{\xi} a_{\xi} \chi^{\xi}$, where $\xi \in \frac{\Theta_F^{\vee}}{3}$. In terms of the local coordinates u_0 and u_1 , we have that $\chi^{\xi z_1 + \tau(\xi) z_2} = u_0^{\operatorname{Tr}(\xi A_0)} u_1^{\operatorname{Tr}(\xi A_1)}$.

The ring $\frac{\Theta_F^{\vee}}{3}$ is spanned by $\frac{1}{3\sqrt{5}}$ and $\frac{\omega}{3\sqrt{5}}$, where $\omega = \frac{1+\sqrt{5}}{2}$. The pull back by the diagonal morphism sends χ^{ξ} to $q^{\operatorname{Tr}(\xi)}$. Hence, $\chi^{\frac{1}{3\sqrt{5}}} = u_0^0 u_1^1$ is sent to $q^0 = 1$ and $\chi^{\frac{\omega}{3\sqrt{5}}} = u_0^1 u_1^2$ is sent to $q^1 = q$. Therefore, the diagonal embedding induces a unique map $\widehat{B} \rightarrow \widehat{A}_{(f)}$. Namely, the map that sends u_0 to q and u_1 to 1. Composing with the map $\operatorname{Spec}(\widehat{B}) \rightarrow \widetilde{\mathcal{H}}(3)$, we obtain a map $\operatorname{Spec}(\widehat{A}_{(f)}) \rightarrow \widetilde{\mathcal{H}}(3)$ compatible with the map $\operatorname{Spec}(A_f) \rightarrow \widetilde{\mathcal{H}}(3)$. By Lemma B.16, the map $\mathcal{U} \setminus \bar{c} \rightarrow \mathcal{H}(3)$ can be extended to a map $\mathcal{U} \rightarrow \mathcal{H}(3)$, completing the proof of the theorem. \square

Theorem B.15 has the following direct consequences. Let $\widetilde{\mathcal{H}}$ be one of the irreducible components of $\widetilde{\mathcal{H}}(3)$ over $\operatorname{Spec} \mathbb{Z}[1/15, \xi_3]$. The set of complex points of $\widetilde{\mathcal{H}}$ agrees with the surface $\widetilde{H}(3)$ of section B.1. Let Z be any irreducible component of the divisor D' of $\widetilde{H}(3)$ introduced in the same section. Then Z is defined over $\mathbb{Q}(\zeta_3)$. Let $\mathcal{Z} = \overline{Z}$ be the Zariski closure of Z in $\widetilde{\mathcal{H}}$.

Corollary B.17. *For every prime \mathfrak{p} of $\mathbb{Z}[1/15, \zeta_3]$, the vertical cycle $\mathcal{Z}_{\mathfrak{p}}$ is irreducible.*

Proof. If Z is a component of S this follows directly from Theorem B.12. If Z is a component of F_1 this follows from Theorem B.15 and Theorem B.13. \square

Let \mathcal{D}' be the horizontal divisor of $\widetilde{\mathcal{H}}$ determined by D .

Corollary B.18. *For every prime \mathfrak{p} of $\mathbb{Z}[1/15, \zeta_3]$, the divisor $\mathcal{D}'_{\mathfrak{p}}$ of the surface $\widetilde{\mathcal{H}}_{\mathfrak{p}}$ over $\text{Spec } \mathbb{Z}[1/15, \zeta_3]/\mathfrak{p}$ is nef.*

Proof. Since the divisor $\mathcal{D}'_{\mathfrak{p}}$ is effective, we only have to show that the intersection of $\mathcal{D}'_{\mathfrak{p}}$ with any of its irreducible components is greater or equal to zero. By Corollary B.17, every irreducible component of $\mathcal{D}'_{\mathfrak{p}}$ is the specialization of a irreducible component of D' . Thus the result follows from the fact that D' is nef and that the intersection product is preserved by specialization. \square

Corollary B.19. *Let G be a Hilbert modular form of weight (k_1, k_2) , with $k_1 \equiv k_2 \pmod{2}$, for $\Gamma_0(3)$ whose coefficients generate a finite field extension L of \mathbb{Q} . Let \mathfrak{p} be a prime ideal of $\mathcal{O}_{L, F[\zeta_3]}$ not dividing 15. If G vanishes with order a at all cusps of $\widetilde{\mathcal{H}}_{\mathfrak{p}}$ and if the Fourier coefficients of its q -expansion at the infinity cusp are algebraic integers satisfying $a_{\xi} \equiv 0 \pmod{\mathfrak{p}}$ for all ξ with $\text{Tr}(\xi) \leq (k_1 + k_2) - 3a$ then all a_{ξ} are divisible by \mathfrak{p} .*

Proof. From the last Corollary, we have that the divisor $\mathcal{D}'_{\mathfrak{p}}$ of the surface $\widetilde{\mathcal{H}}_{\mathfrak{p}}$ over $\text{Spec } \mathbb{Z}[1/15, \zeta_3]/\mathfrak{p}$ is nef, so we can apply the same argument as in the proof of Theorems B.3 and B.6. The result follows from the fact that $\mathcal{D}'_{\mathfrak{p}}$ is the specialization of the divisor D consider in such theorems and the fact that intersection numbers are preserved by specialization. \square

Remark B.20. In practice, if one starts with a form whose coefficients vanish at all cusps of the complex Hilbert surface with order at least a (for example if it is a product of cusp forms, as will be the case in the next section) then it also vanishes at all the cusps of $\widetilde{\mathcal{H}}_{\mathfrak{p}}$ with order at least a .

B.3. The case the form $(f + \tau(f)) \otimes \chi_{\sqrt{5}}$ of level $\Gamma_0(6\sqrt{5})$. We want to apply the results of the last two sections to the twist of the Hilbert cusp form $f + \tau(f)$ of Section 2, which has of weight $(2, 4)$ and level $\Gamma_0(6\sqrt{5})$. Assuming that its q -expansion at the infinity cusp is zero for all elements of trace smaller than $\tilde{b} + 1$ (hence the order of vanishing at the four lines L_i , $i = 1, \dots, 3$ is $3\tilde{b} + 3$), we want to determine which value of \tilde{b} forces the form to be the zero form. We start with some general results.

Lemma B.21. *Let \mathfrak{p} be a prime ideal of F , then the finite group $\text{SL}_2(\mathcal{O}_F/\mathfrak{p}^r)$ has $N\mathfrak{p}^r N\mathfrak{p}^{2(r-1)}(N\mathfrak{p} - 1)(N\mathfrak{p} + 1)$ elements, and the subgroup of upper triangular matrices has $N\mathfrak{p}^r N\mathfrak{p}^{r-1}(N\mathfrak{p} - 1)$ elements.*

Proof. This is elementary, one way of doing it is by counting the disjoint cases where \mathfrak{p} divides the $(1, 1)$ place of the matrix and where it does not, and put one entry in terms of the others. The second statement is trivial. \square

In particular the quotient of the two groups has order $\mathcal{N}\mathfrak{p}^{r-1}(\mathcal{N}\mathfrak{p} + 1)$. A set of representatives for the quotient is given by

$$(11) \quad \left\{ \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & \beta \end{pmatrix} \right\},$$

where α runs through a set of representatives of $(\mathfrak{p}/\mathfrak{p}^r)$ and β runs over a set of representatives of $(\mathcal{O}_F/\mathfrak{p}^r)$ (just by checking that these elements are not equivalent).

Lemma B.22. *Let $\mathfrak{p}, \mathfrak{q}$ be two distinct prime ideals of F relatively prime to 3. Then the index of $\Gamma_0(3\mathfrak{p}^r\mathfrak{q}^s)$ in $\Gamma_0(3)$ is*

$$[\Gamma_0(3) : \Gamma_0(3\mathfrak{p}^r\mathfrak{q}^s)] = \mathcal{N}\mathfrak{p}^{r-1}(\mathcal{N}\mathfrak{p} + 1)\mathcal{N}\mathfrak{q}^{s-1}(\mathcal{N}\mathfrak{q} + 1).$$

Proof. This is a standard computation. Since these subgroups only differ at the primes \mathfrak{p} and \mathfrak{q} , we can consider the morphism

$$\mathrm{SL}_2(\mathcal{O}_F) \mapsto \mathrm{SL}_2(\mathcal{O}_F/\mathfrak{p}^r) \times \mathrm{SL}_2(\mathcal{O}_F/\mathfrak{q}^s).$$

The group $\Gamma_0(3)$ surjects into this product (by the Chinese remainder theorem), while the group $\Gamma_0(3\mathfrak{p}^r\mathfrak{q}^s)$ maps to the upper triangular matrices. The statement thus follows from Lemma B.21. \square

In particular,

$$(12) \quad [\Gamma_0(3) : \Gamma_0(6\sqrt{5})] = 30.$$

We can also give the number of cusps and representatives for them.

Lemma B.23. *Let \mathfrak{p} be a prime ideal of F . The number of non-equivalent cusps for $\Gamma_0(\mathfrak{p})$ is 2.*

Proof. Since F has class number one, the same computations as for the classical case work, and there are two non-equivalent classes for the prime ideal \mathfrak{p} which are the sets

$$C_1^{\mathfrak{p}} = \left\{ \frac{a}{b} \in F : \mathfrak{p} \mid b \right\}$$

$$C_2^{\mathfrak{p}} = \left\{ \frac{a}{b} \in F : \mathfrak{p} \nmid b \right\},$$

They are usually denoted by the class of ∞ (corresponding to the element $\frac{a}{0}$) and the class of 0. \square

Remark B.24. It follows from the above description of the set of equivalent cusps and the Chinese remainder Theorem that the number of non-equivalent cusps is multiplicative, i.e. if $\mathfrak{n}, \mathfrak{m}$ are two different ideals of F prime to each other, and cubic free, then the number of non-equivalent cusps for $\Gamma_0(\mathfrak{nm})$ is the product of the number of non-equivalent cusps for $\Gamma_0(\mathfrak{n})$ times the number for $\Gamma_0(\mathfrak{m})$.

Let \mathfrak{h} be the modular form of weight $(6, 6)$ for $\Gamma_0(6\sqrt{5})$ defined by

$$(13) \quad \mathfrak{h} = (\mathfrak{f}(z_1, z_2) + \tau(\mathfrak{f}(z_1, z_2))) \otimes \chi_{\sqrt{5}} \cdot (\mathfrak{f}(z_2, z_1) + \tau(\mathfrak{f}(z_2, z_1))) \otimes \chi_{\sqrt{5}}.$$

It vanishes with order 2 at all cusps, and with order $2\tilde{b} + 2$ at the infinity cusp. Let

$$G := \prod_{\gamma \in \Gamma_0(6\sqrt{5}) \backslash \Gamma_0(3)} \mathfrak{h}|_6[\gamma].$$

It is a parallel weight $6 \cdot 30$ Hilbert modular form for $\Gamma_0(3)$. We need to compute the order of vanishing of G at the different cusps. By definition,

$$(14) \quad G = \prod_{\gamma_1 \in \Gamma_0(6) \backslash \Gamma_0(3)} \left(\prod_{\gamma_2 \in \Gamma_0(6\sqrt{5}) \backslash \Gamma_0(6)} \mathfrak{h}|_6[\gamma_1 \gamma_2] \right).$$

The group $\Gamma_0(6)$ has 4 non-equivalent cusps, while the group $\Gamma_0(6\sqrt{5})$ has 8 such cusps. They are given by the elements $C_\alpha^2 \cap C_\beta^3 \cap D_\gamma^{\sqrt{5}}$, where $(\alpha, \beta, \gamma) \in \{1, 2\} \times \{1, 2\} \times \{1, 2\}$. If $\gamma = 1$, then any form of level $\Gamma_0(6\sqrt{5})$ at a cusp of $C_\alpha^2 \cap C_\beta^3 \cap D_\gamma^{\sqrt{5}}$ has a q -expansion of the form

$$(15) \quad \sum_{\substack{\xi \gg 0 \\ \xi \in \frac{\mathcal{O}_F}{\sqrt{5}} 2^{1-\alpha} 3^{1-\beta}}} a_\xi \exp(\xi z_1 + \tau(\xi) z_2),$$

since in this case an element congruent to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ modulo $5\mathcal{O}_F$ is in the stabilizer of the cusp. In the other cases, the q -expansion has the form

$$(16) \quad \sum_{\substack{\xi \gg 0 \\ \xi \in \frac{\mathcal{O}_F}{\sqrt{5}} 2^{1-\alpha} 3^{1-\beta}}} a_\xi \exp(\xi z_1 + \tau(\xi) z_2).$$

The second product of equation (14) has 6 terms, and considering the representatives for the quotient given in (11), it is easy to see that the terms involved in the product correspond to 1 terms with $\gamma = 1$ and 5 terms with $\gamma = 2$ (and all of them have the same value of α and β). Since our form \mathfrak{h} is a cusp form, the 0 term and the term with minimum trace in the q -expansion vanish, hence the trace of the first product of equation (14) at the cusp (α, β) is bounded below by

$$\begin{cases} 2 \cdot 2 \cdot 2^{1-\alpha} \cdot 3^{1-\beta} & \text{if } (\alpha, \beta) \neq (1, 1) \\ 2\tilde{b} + 4 & \text{if } (\alpha, \beta) = (1, 1). \end{cases}$$

The same reasoning for the second product (which has 5 terms) gives that 4 of the terms have q -expansion corresponding to $\alpha = 2$ and 1 term with $\alpha = 1$. We obtain that the trace of the q -expansion of G is bounded below by

$$\begin{cases} 4 & \text{if } \beta \neq 1 \\ 2\tilde{b} + 12 & \text{if } \beta = 1. \end{cases}$$

Since the order of vanishing at the infinity cusp is three times the trace of the first non-zero element (because our form is a form for $\Gamma_0(3)$ rather than $\Gamma(3)$), Theorem B.3 and Corollary B.19 (with $a = 4$, $b = 6\tilde{b} + 32$ and $k = 90$) imply that if $\tilde{b} \geq 168$ then G is the zero form. So we get

Theorem B.25. *Let \mathfrak{h} be a Hilbert modular form of parallel weight $(2, 4)$ for $\Gamma_0(6\sqrt{5})$. If its Fourier expansion is given by*

$$\mathfrak{h} = \sum_{\substack{\xi \gg 0 \\ \xi \in \mathcal{O}_F^\vee}} a_\xi \exp(\xi z_1 + \tau(\xi) z_2).$$

with $a_\xi \equiv 0 \pmod{2}$ for all ξ with $\text{Tr}(\xi) \leq 168$, then $a_\xi \equiv 0 \pmod{2}$ for all ξ .

REFERENCES

- [BBGK07] Jan H. Bruinier, José I. Burgos Gil, and Ulf Kühn. Borchers products and arithmetic intersection theory on Hilbert modular surfaces. *Duke Math. J.*, 139(1):1–88, 2007.
- [Car86] Henri Carayol. Sur les représentations l -adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)*, 19(3):409–468, 1986.
- [Cha90] C.-L. Chai. Arithmetic minimal compactification of the Hilbert-Blumenthal moduli spaces. *Ann. of Math. (2)*, 131(3):541–554, 1990.
- [Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
- [CS01] Caterina Consani and Jasper Scholten. Arithmetic on a quintic threefold. *Internat. J. Math.*, 12(8):943–972, 2001.
- [DD06] Luis Dieulefait and Mladen Dimitrov. Explicit determination of images of Galois representations attached to Hilbert modular forms. *J. Number Theory*, 117(2):397–405, 2006.
- [DGP] Luis Dieulefait, Lucio Guerberooff, and Ariel Pacetti. Proving modularity for a given elliptic curve over an imaginary quadratic field. *Math. Comp. (electronically posted on August 4, 2009)*.
- [Dim09] Mladen Dimitrov. On Ihara’s lemma for Hilbert modular varieties. *Compos. Math.*, 145(5):1114–1146, 2009.
- [DM03] Luis Dieulefait and Jayanta Manoharmayum. Modularity of rigid Calabi-Yau threefolds over Q . In *Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001)*, volume 38 of *Fields Inst. Commun.*, pages 159–166. Amer. Math. Soc., Providence, RI, 2003.
- [DPS] Luis Dieulefait, Ariel Pacetti, and Matthias Schütt. Table of eigenvalues of a hilbert modular form. Available from http://www.iag.uni-hannover.de/~schuett/publik_en.html.

- [DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.
- [Gor02] Eyal Z. Goren. *Lectures on Hilbert modular varieties and modular forms*, volume 14 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2002. With the assistance of Marc-Hubert Nicole.
- [HV06] K. Hulek and H. Verrill. On the modularity of Calabi-Yau threefolds containing elliptic ruled surfaces. In *Mirror symmetry. V*, volume 38 of *AMS/IP Stud. Adv. Math.*, pages 19–34. Amer. Math. Soc., Providence, RI, 2006. With an appendix by Luis V. Dieulefait.
- [KW09a] Chandrashekhhar Khare and Jean-Pierre Wintenberger. Serre’s modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.
- [KW09b] Chandrashekhhar Khare and Jean-Pierre Wintenberger. Serre’s modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.
- [Liv87] Ron Livné. Cubic exponential sums and Galois representations. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, volume 67 of *Contemp. Math.*, pages 247–261. Amer. Math. Soc., Providence, RI, 1987.
- [PAR08] The PARI Group, Bordeaux. *PARI/GP, version 2.4.3*, 2008. available from <http://pari.math.u-bordeaux.fr/>.
- [Rap78] M. Rapoport. Compactifications de l’espace de modules de Hilbert-Blumenthal. *Compositio Math.*, 36(3):255–335, 1978.
- [SGA03] *Revêtements étales et groupe fondamental (SGA 1)*. Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3. Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960–61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)].
- [Tay89] Richard Taylor. On Galois representations associated to Hilbert modular forms. *Invent. Math.*, 98(2):265–280, 1989.
- [vdG88] Gerard van der Geer. *Hilbert modular surfaces*, volume 16 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988.

LUIS DIEULEFAIT
DEPARTAMENT D'ÀLGEBRA I GEOMETRIA
FACULTAT DE MATEMÀTIQUES
UNIVERSITAT DE BARCELONA
GRAN VIA DE LES CORTS CATALANES, 585
08007 BARCELONA
E-mail address: `ldieulefait@ub.edu`

ARIEL PACETTI
DEPARTAMENTO DE MATEMÁTICA
UNIVERSIDAD DE BUENOS AIRES
PABELLÓN I, CIUDAD UNIVERSITARIA
C.P:1428, BUENOS AIRES, ARGENTINA
E-mail address: `apacetti@dm.uba.ar`

MATTHIAS SCHÜTT
INSTITUT FÜR ALGEBRAISCHE GEOMETRIE
LEIBNIZ UNIVERSITÄT HANNOVER
WELFENGARTEN 1
30167 HANNOVER, GERMANY
E-mail address: `schuett@math.uni-hannover.de`

ICMAT-CSIC
E-mail address: `jiburgosgil@gmail.com`